Cartilha de Segurança para Internet

Publicação cert.br



http://cartilha.cert.br/

nic.br cgi.br

Núcleo de Informação e Coordenação do Ponto BR
Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Versão 4.0

Comitê Gestor da Internet no Brasil

São Paulo
2012

Comitê Gestor da Internet no Brasil (CGI.br)
Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)

Textos e Edição: Equipe do CERT.br
Ilustrações: Héctor Gómez e Osnei

Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

Primeira edição: 2006
ISBN: 978-85-60062-05-8
ISBN: 85-60062-05-X

Segunda edição: 2012
ISBN: 978-85-60062-54-6

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários para se protegerem destas ameaças.

A produção desta Cartilha foi feita pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é um dos serviços prestados para a comunidade Internet do Brasil pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), o braço executivo do Comitê Gestor da Internet no Brasil (CGI.br).

Nós esperamos que esta Cartilha possa auxiliá-lo não só a compreender as ameaças do ambiente Internet, mas também a usufruir dos benefícios de forma consciente e a manter a segurança de seus dados, computadores e dispositivos móveis. Gostaríamos ainda de ressaltar que é muito importante ficar sempre atento ao usar a Internet, pois somente aliando medidas técnicas a boas práticas é possível atingir um nível de segurança que permita o pleno uso deste ambiente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, por favor, entre em contato por meio do endereço `doc@cert.br`.

Boa leitura!

Equipe do CERT.br
Junho de 2012

Estrutura da Cartilha

Este documento conta com quatorze capítulos, que dividem o conteúdo em diferentes áreas relacionadas com a segurança da Internet, além de um glossário e um índice remissivo.

De forma geral, o Capítulo 1 apresenta uma introdução sobre a importância de uso da Internet, os riscos a que os usuários estão sujeitos e os cuidados a serem tomados. Do Capítulo 2 ao 6 os riscos são apresentados de forma mais detalhada, enquanto que do Capítulo 7 ao 14 o foco principal são os cuidados a serem tomados e os mecanismos de segurança existentes.

1. **Segurança na Internet:** Trata dos benefícios que a Internet pode trazer na realização de atividades cotidianas e descreve, de forma geral, os riscos relacionados ao seu uso. Procura também esclarecer que a Internet não tem nada de "virtual" e que os cuidados a serem tomados ao usá-la são semelhantes aos que se deve ter no dia a dia.

2. Golpes na Internet: Apresenta os principais golpes aplicados na Internet, os riscos que estes golpes representam e os cuidados que devem ser tomados para se proteger deles.

3. Ataques na Internet: Aborda os ataques que costumam ser realizados por meio da Internet, as motivações que levam os atacantes a praticar atividades deste tipo e as técnicas que costumam ser utilizadas. Ressalta a importância de cada um fazer a sua parte para que a segurança geral da Internet possa ser melhorada.

4. Códigos maliciosos (*Malware*): Aborda os diferentes tipos de códigos maliciosos, as diversas formas de infecção e as principais ações danosas e atividades maliciosas por eles executadas. Apresenta também um resumo comparativo para facilitar a classificação dos diferentes tipos.

5. *Spam*: Discute os problemas acarretados pelo *spam*, principalmente aqueles que possam ter implicações de segurança, e métodos de prevenção.

6. Outros riscos: Aborda alguns dos serviços e recursos de navegação incorporados a grande maioria dos navegadores *Web* e leitores de *e-mails*, os riscos que eles podem representar e os cuidados que devem ser tomados ao utilizá-los. Trata também dos riscos apresentados e dos cuidados a serem tomados ao compartilhar recursos na Internet.

7. Mecanismos de segurança: Apresenta os principais mecanismos de segurança existentes e os cuidados que devem ser tomados ao utilizá-los. Ressalta a importância de utilização de ferramentas de segurança aliada a uma postura preventiva.

8. Contas e senhas: Aborda o principal mecanismo de autenticação usado na Internet que são as contas e as senhas. Inclui dicas de uso, elaboração, gerenciamento, alteração e recuperação, entre outras.

9. Criptografia: Apresenta alguns conceitos de criptografia, como funções de resumo, assinatura digital, certificado digital e as chaves simétricas e assimétricas. Trata também dos cuidados que devem ser tomados ao utilizá-la.

10. Uso seguro da Internet: Apresenta, de forma geral, os principais usos que são feitos da Internet e os cuidados que devem ser tomados ao utilizá-los. Aborda questões referentes a segurança nas conexões *Web* especialmente as envolvem o uso de certificados digitais.

11. Privacidade: Discute questões relacionadas à privacidade do usuário ao utilizar a Internet e aos cuidados que ele deve ter com seus dados pessoais. Apresenta detalhadamente dicas referentes a disponibilização de informações pessoais nas redes sociais.

12. Segurança de computadores: Apresenta os principais cuidados que devem ser tomados ao usar computadores, tanto pessoais como de terceiros. Ressalta a importância de manter os computadores atualizados e com mecanismos de proteção instalados.

13. Segurança de redes: Apresenta os riscos relacionados ao uso das principais tecnologias de acesso à Internet, como banda larga (fixa e móvel), Wi-Fi e *Bluetooth*.

14. Segurança em dispositivos móveis: Aborda os riscos relacionados ao uso de dispositivos móveis e procura demonstrar que eles são similares aos computadores e que, por isto, necessitam dos mesmos cuidados de segurança.

Licença de Uso da Cartilha

Histórico da Cartilha

No início de 2000, um grupo de estudos que, entre outros, envolveu a Abranet e o CERT.br (que à época chamava-se NBSO – NIC BR Security Office), identificou a necessidade de um guia com informações sobre segurança que pudesse ser usado como referência pelos diversos setores usuários de Internet. Como conseqüência, a pedido do Comitê Gestor da Internet no Brasil e sob supervisão do CERT.br, em julho do mesmo ano foi lançada a Cartilha de Segurança para Internet Versão 1.0.

Em 2003 foi verificada a necessidade de uma revisão geral do documento, que não só incluísse novos tópicos, mas que também facilitasse sua leitura e a localização de assuntos específicos. Neste processo de revisão a Cartilha foi completamente reescrita, dando origem à versão 2.0. Esta versão, a primeira totalmente sob responsabilidade do CERT.br, possuía estrutura dividida em partes, além de contar com o *checklist* e o glossário. Também nesta versão foram introduzidas as seções relativas a fraudes na Internet, banda larga, redes sem fio, *spam* e incidentes de segurança.

Na versão 3.0, de 2005, a Cartilha continuou com sua estrutura, mas, devido à evolução da tecnologia, novos assuntos foram incluídos. Foi criada uma parte específica sobre códigos maliciosos, expandida a parte sobre segurança de redes sem fio e incluídos tópicos específicos sobre segurança em dispositivos móveis. Esta versão também foi a primeira a disponibilizar um folheto com as dicas básicas para proteção contra as ameaças mais comuns.

A versão 3.1 não introduziu partes novas, mas incorporou diversas sugestões de melhoria recebidas, corrigiu alguns erros de digitação e atendeu a um pedido de muitos leitores: lançá-la em formato de livro, para facilitar a leitura e a impressão do conteúdo completo.

Em 2012 foi verificada novamente a necessidade de revisão geral do documento, o que deu origem à versão 4.0. Com o uso crescente da Internet e das redes sociais, impulsionado principalmente pela popularização dos dispositivos móveis e facilidades de conexão, constatou-se a necessidade de abordar novos conteúdos e agrupar os assuntos de maneira diferente. Esta versão conta com um livro com todo o conteúdo que, com o objetivo de facilitar a leitura e torná-la mais agradável, é totalmente ilustrado. Este livro, por sua vez, é complementado por fascículos com versões resumidas de alguns dos tópicos, de forma a facilitar a difusão de conteúdos específicos.

Agradecimentos

Agradecemos a todos leitores da Cartilha, que têm contribuído para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.

Agradecemos as contribuições de Rafael Rodrigues Obelheiro, na versão 3.0, e de Nelson Murilo, na Parte V da versão 3.1 e no Capítulo 13 da atual versão.

Agradecemos a toda equipe do CERT.br, especialmente a Luiz E. R. Cordeiro, pelo texto da primeira versão; a Marcelo H. P. C. Chaves, pela produção das versões 2.0, 3.0 e 3.1 e pela criação das figuras da atual versão; a Lucimara Desiderá, pelas pesquisas realizadas, pela contribuição nos Capítulos 9 e 13 e também pela pela criação das figuras da atual versão; e a Miriam von Zuben, pela produção da versão 4.0 e por ser a principal mantenedora da Cartilha.

Sumário

Lista de Figuras

Lista de Tabelas

1. Segurança na Internet



A Internet já está presente no cotidiano de grande parte da população e, provavelmente para estas pessoas, seria muito difícil imaginar como seria a vida sem poder usufruir das diversas facilidades e oportunidades trazidas por esta tecnologia. Por meio da Internet você pode:

- encontrar antigos amigos, fazer novas amizades, encontrar pessoas que compartilham seus gostos e manter contato com amigos e familiares distantes;
- acessar *sites* de notícias e de esportes, participar de cursos à distância, pesquisar assuntos de interesse e tirar dúvidas em listas de discussão;
- efetuar serviços bancários, como transferências, pagamentos de contas e verificação de extratos;
- fazer compras em supermercados e em lojas de comércio eletrônico, pesquisar preços e verificar a opinião de outras pessoas sobre os produtos ou serviços ofertados por uma determinada loja;
- acessar *sites* dedicados a brincadeiras, passatempos e histórias em quadrinhos, além de grande variedade de jogos, para as mais diversas faixas etárias;
- enviar a sua declaração de Imposto de Renda, emitir boletim de ocorrência, consultar os pontos em sua carteira de habilitação e agendar a emissão de passaporte;

- consultar a programação das salas de cinema, verificar a agenda de espetáculos teatrais, exposições e *shows* e adquirir seus ingressos antecipadamente;
- consultar acervos de museus e *sites* dedicados à obra de grandes artistas, onde é possível conhecer a biografia e as técnicas empregadas por cada um.

Estes são apenas alguns exemplos de como você pode utilizar a Internet para facilitar e melhorar a sua vida. Aproveitar esses benefícios de forma segura, entretanto, requer que alguns cuidados sejam tomados e, para isto, é importante que você esteja informado dos riscos aos quais está exposto para que possa tomar as medidas preventivas necessárias. Alguns destes riscos são:

Acesso a conteúdos impróprios ou ofensivos: ao navegar você pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo.

Contato com pessoas mal-intencionadas: existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro.

Furto de identidade: assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputação.

Furto e perda de dados: os dados presentes em seus equipamentos conectados à Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos.

Invasão de privacidade: a divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não serão repassadas. Além disto, os *sites* costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado.

Divulgação de boatos: as informações na Internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo. Enquanto isto pode ser desejável em certos casos, também pode ser usado para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.

Dificuldade de exclusão: aquilo que é divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado. Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você e acessada por diferentes pessoas, desde seus familiares até seus chefes.

Dificuldade de detectar e expressar sentimentos: quando você se comunica via Internet não há como observar as expressões faciais ou o tom da voz das outras pessoas, assim como elas não podem observar você (a não ser que vocês estejam utilizando *webcams* e microfones). Isto pode dificultar a percepção do risco, gerar mal-entendido e interpretação dúbia.

Dificuldade de manter sigilo: no seu dia a dia é possível ter uma conversa confidencial com alguém e tomar cuidados para que ninguém mais tenha acesso ao que está sendo dito. Na Internet, caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo.

Uso excessivo: o uso desmedido da Internet, assim como de outras tecnologias, pode colocar em risco a sua saúde física, diminuir a sua produtividade e afetar a sua vida social ou profissional.

Plágio e violação de direitos autorais: a cópia, alteração ou distribuição não autorizada de conteúdos e materiais protegidos pode contrariar a lei de direitos autorais e resultar em problemas jurídicos e em perdas financeiras.

Outro grande risco relacionado ao uso da Internet é o de você achar que não corre riscos, pois supõe que ninguém tem interesse em utilizar o seu computador[1] ou que, entre os diversos computadores conectados à Internet, o seu dificilmente será localizado. É justamente este tipo de pensamento que é explorado pelos atacantes, pois, ao se sentir seguro, você pode achar que não precisa se prevenir.

Esta ilusão, infelizmente, costuma terminar quando os primeiros problemas começam a acontecer. Muitas vezes os atacantes estão interessados em conseguir acesso a grandes quantidades de computadores, independente de quais são, e para isto, podem efetuar varreduras na rede e localizar grande parte dos computadores conectados à Internet, inclusive o seu.

Um problema de segurança em seu computador pode torná-lo indisponível e colocar em risco a confidencialidade e a integridade dos dados nele armazenados. Além disto, ao ser comprometido, seu computador pode ser usado para a prática de atividades maliciosas como, por exemplo, servir de repositório para dados fraudulentos, lançar ataques contra outros computadores (e assim esconder a real identidade e localização do atacante), propagar códigos maliciosos e disseminar *spam*.

Os principais riscos relacionados ao uso da Internet são detalhados nos Capítulos: Golpes na Internet, Ataques na Internet, Códigos maliciosos (*Malware*), *Spam* e Outros riscos.

O primeiro passo para se prevenir dos riscos relacionados ao uso da Internet é estar ciente de que ela não tem nada de "virtual". Tudo o que ocorre ou é realizado por meio da Internet é real: os dados são reais e as empresas e pessoas com quem você interage são as mesmas que estão fora dela. Desta forma, os riscos aos quais você está exposto ao usá-la são os mesmos presentes no seu dia a dia e os golpes que são aplicados por meio dela são similares àqueles que ocorrem na rua ou por telefone.

É preciso, portanto, que você leve para a Internet os mesmos cuidados e as mesmas preocupações que você tem no seu dia a dia, como por exemplo: visitar apenas lojas confiáveis, não deixar públicos dados sensíveis, ficar atento quando "for ao banco" ou "fizer compras", não passar informações a estranhos, não deixar a porta da sua casa aberta, etc.

Para tentar reduzir os riscos e se proteger é importante que você adote uma postura preventiva e que a atenção com a segurança seja um hábito incorporado à sua rotina, independente de questões como local, tecnologia ou meio utilizado. Para ajudá-lo nisto, há diversos mecanismos de segurança que você pode usar e que são detalhados nos Capítulos: Mecanismos de segurança, Contas e senhas e Criptografia.

Outros cuidados, relativos ao uso da Internet, como aqueles que você deve tomar para manter a sua privacidade e ao utilizar redes e dispositivos móveis, são detalhados nos demais Capítulos: Uso seguro da Internet, Privacidade, Segurança de computadores, Segurança de redes e Segurança em dispositivos móveis.

[1]Nesta Cartilha a palavra "computador" será usada para se referir a todos os dispositivos computacionais passíveis de invasão e/ou de infecção por códigos maliciosos, como computadores e dispositivos móveis.

2. Golpes na Internet



Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários. Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

De posse dos dados das vítimas, os golpistas costumam efetuar transações financeiras, acessar *sites*, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas.

Muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato. Dessa forma, o golpista pode ser considerado um estelionatário.

Nas próximas seções são apresentados alguns dos principais golpes aplicados na Internet e alguns cuidados que você deve tomar para se proteger deles.

2.1 Furto de identidade (*Identity theft*)

O furto de identidade, ou *identity theft*, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de *e-mail* e envie mensagens se passando por você ou falsifique os campos de *e-mail*, fazendo parecer que ele foi enviado por você.

Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar a sua identidade, pois mais dados ele tem disponíveis e mais convincente ele pode ser. Além disto, o golpista pode usar outros tipos de golpes e ataques para coletar informações sobre você, inclusive suas senhas, como códigos maliciosos (mais detalhes no Capítulo Códigos maliciosos (*Malware*)), ataques de força bruta e interceptação de tráfego (mais detalhes no Capítulo Ataques na Internet).

Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito. Além disto, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

Prevenção:

A melhor forma de impedir que sua identidade seja furtada é evitar que o impostor tenha acesso aos seus dados e às suas contas de usuário (mais detalhes no Capítulo Privacidade). Além disto, para evitar que suas senhas sejam obtidas e indevidamente usadas, é muito importante que você seja cuidadoso, tanto ao usá-las quanto ao elaborá-las (mais detalhes no Capítulo Contas e senhas).

É necessário também que você fique atento a alguns indícios que podem demonstrar que sua identidade está sendo indevidamente usada por golpistas, tais como:

- você começa a ter problemas com órgãos de proteção de crédito;
- você recebe o retorno de *e-mails* que não foram enviados por você;
- você verifica nas notificações de acesso que a sua conta de *e-mail* ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando;
- ao analisar o extrato da sua conta bancária ou do seu cartão de crédito você percebe transações que não foram realizadas por você;
- você recebe ligações telefônicas, correspondências e *e-mails* se referindo a assuntos sobre os quais você não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por você.

2.2 Fraude de antecipação de recursos (*Advance fee fraud*)

A fraude de antecipação de recursos, ou *advance fee fraud*, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Por meio do recebimento de mensagens eletrônicas ou do acesso a *sites* fraudulentos, a pessoa é envolvida em alguma situação ou história mirabolante, que justifique a necessidade de envio de informações pessoais ou a realização de algum pagamento adiantado, para a obtenção de um benefício futuro. Após fornecer os recursos solicitados a pessoa percebe que o tal benefício prometido não existe, constata que foi vítima de um golpe e que seus dados/dinheiro estão em posse de golpistas.

O Golpe da Nigéria (*Nigerian 4-1-9 Scam*[1]) é um dos tipos de fraude de antecipação de recursos mais conhecidos e é aplicado, geralmente, da seguinte forma:

a. Você recebe uma mensagem eletrônica em nome de alguém ou de alguma instituição dizendo-se ser da Nigéria, na qual é solicitado que você atue como intermediário em uma transferência internacional de fundos;

b. o valor citado na mensagem é absurdamente alto e, caso você aceite intermediar a transação, recebe a promessa de futuramente ser recompensado com uma porcentagem deste valor;

c. o motivo, descrito na mensagem, pelo qual você foi selecionado para participar da transação geralmente é a indicação de algum funcionário ou amigo que o apontou como sendo uma pessoa honesta, confiável e merecedora do tal benefício;

d. a mensagem deixa claro que se trata de uma transferência ilegal e, por isto, solicita sigilo absoluto e urgência na resposta, caso contrário, a pessoa procurará por outro parceiro e você perderá a oportunidade;

e. após responder a mensagem e aceitar a proposta, os golpistas solicitam que você pague antecipadamente uma quantia bem elevada (porém bem inferior ao total que lhe foi prometido) para arcar com custos, como advogados e taxas de transferência de fundos;

f. após informar os dados e efetivar o pagamento solicitado, você é informado que necessita realizar novos pagamentos ou perde o contato com os golpistas;

g. finalmente, você percebe que, além de perder todo o dinheiro investido, nunca verá a quantia prometida como recompensa e que seus dados podem estar sendo indevidamente usados.

Apesar deste golpe ter ficado conhecido como sendo da Nigéria, já foram registrados diversos casos semelhantes, originados ou que mencionavam outros países, geralmente de regiões pobres ou que estejam passando por conflitos políticos, econômicos ou raciais.

A fraude de antecipação de recursos possui diversas variações que, apesar de apresentarem diferentes discursos, assemelham-se pela forma como são aplicadas e pelos danos causados. Algumas destas variações são:

[1]O número 419 refere-se à seção do Código Penal da Nigéria equivalente ao artigo 171 do Código Penal Brasileiro, ou seja, estelionato.

Loteria internacional: você recebe um *e-mail* informando que foi sorteado em uma loteria internacional, mas que para receber o prêmio a que tem direito, precisa fornecer seus dados pessoais e informações sobre a sua conta bancária.

Crédito fácil: você recebe um *e-mail* contendo uma oferta de empréstimo ou financiamento com taxas de juros muito inferiores às praticadas no mercado. Após o seu crédito ser supostamente aprovado você é informado que necessita efetuar um depósito bancário para o ressarcimento das despesas.

Doação de animais: você deseja adquirir um animal de uma raça bastante cara e, ao pesquisar por possíveis vendedores, descobre que há *sites* oferecendo estes animais para doação. Após entrar em contato, é solicitado que você envie dinheiro para despesas de transporte.

Oferta de emprego: você recebe uma mensagem em seu celular contendo uma proposta tentadora de emprego. Para efetivar a contratação, no entanto, é necessário que você informe detalhes de sua conta bancária.

Noiva russa: alguém deixa um recado em sua rede social contendo insinuações sobre um possível relacionamento amoroso entre vocês. Esta pessoa mora em outro país, geralmente a Rússia, e após alguns contatos iniciais sugere que vocês se encontrem pessoalmente, mas, para que ela possa vir até o seu país, necessita ajuda financeira para as despesas de viagem.

Prevenção:

A melhor forma de se prevenir é identificar as mensagens contendo tentativas de golpes. Uma mensagem deste tipo, geralmente, possui características como:

- oferece quantias astronômicas de dinheiro;
- solicita sigilo nas transações;
- solicita que você a responda rapidamente;
- apresenta palavras como "urgente" e "confidencial" no campo de assunto;
- apresenta erros gramaticais e de ortografia (muitas mensagens são escritas por meio do uso de programas tradutores e podem apresentar erros de tradução e de concordância).

Além disto, adotar uma postura preventiva pode, muitas vezes, evitar que você seja vítima de golpes. Por isto, é muito importante que você:

- questione-se por que justamente você, entre os inúmeros usuários da Internet, foi escolhido para receber o benefício proposto na mensagem e como chegaram até você;
- desconfie de situações onde é necessário efetuar algum pagamento com a promessa de futuramente receber um valor maior (pense que, em muitos casos, as despesas poderiam ser descontadas do valor total).

Aplicar a sabedoria popular de ditados como "Quando a esmola é demais, o santo desconfia" ou "Tudo que vem fácil, vai fácil", também pode ajudá-lo nesses casos.

Vale alertar que mensagens deste tipo nunca devem ser respondidas, pois isto pode servir para confirmar que o seu endereço de *e-mail* é válido. Esta informação pode ser usada, por exemplo, para incluí-lo em listas de *spam* ou de possíveis vítimas em outros tipos de golpes.

2.3 *Phishing*



Phishing[2], *phishing-scam* ou *phishing/scam*, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

O *phishing* ocorre por meio do envio de mensagens eletrônicas que:

- tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um *site* popular;
- procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas *Web*.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento, como exemplificado na Tabela 2.1[3]. Exemplos de situações envolvendo *phishing* são:

Páginas falsas de comércio eletrônico ou *Internet Banking*: você recebe um *e-mail*, em nome de um *site* de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um *link*. Ao fazer isto, você é direcionado para uma página *Web* falsa, semelhante ao *site* que você realmente deseja acessar, onde são solicitados os seus dados pessoais e financeiros.

Páginas falsas de redes sociais ou de companhias aéreas: você recebe uma mensagem contendo um *link* para o *site* da rede social ou da companhia aérea que você utiliza. Ao clicar, você é direcionado para uma página *Web* falsa onde é solicitado o seu nome de usuário e a sua senha que, ao serem fornecidos, serão enviados aos golpistas que passarão a ter acesso ao *site* e poderão efetuar ações em seu nome, como enviar mensagens ou emitir passagens aéreas.

Mensagens contendo formulários: você recebe uma mensagem eletrônica contendo um formulário com campos para a digitação de dados pessoais e financeiros. A mensagem solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações. Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.

Mensagens contendo *links* para códigos maliciosos: você recebe um *e-mail* que tenta induzi-lo a clicar em um *link*, para baixar e abrir/executar um arquivo. Ao clicar, é apresentada uma mensagem de erro ou uma janela pedindo que você salve o arquivo. Após salvo, quando você abri-lo/executá-lo, será instalado um código malicioso em seu computador.

[2]A palavra *phishing*, do inglês "*fishing*", vem de uma analogia criada pelos fraudadores, onde "iscas" (mensagens eletrônicas) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

[3]Esta lista não é exaustiva e nem se aplica a todos os casos, pois ela pode variar conforme o destaque do momento.

Solicitação de recadastramento: você recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de *e-mail* está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que você forneça seus dados pessoais, como nome de usuário e senha.

Tópico	Tema da mensagem
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, *Voxcards*, Yahoo! Cartões, O Carteiro, *Emotioncard*
Comércio eletrônico	cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em *site* de compras coletivas
Companhias aéreas	promoção, programa de milhagem
Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	nova versão ou correção de programa consulta de restituição, problema nos dados da declaração
Internet Banking	unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Músicas	canção dedicada por amigos
Notícias e boatos	fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	loteria, instituição financeira
Programas em geral	lançamento de nova versão ou de novas funcionalidades
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	produto, curso, treinamento, concurso
Reality shows	Big Brother Brasil, A Fazenda, Ídolos
Redes sociais	notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	recebimento de telegrama *online*
Serviços de *e-mail*	recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos
Sites com dicas de segurança	aviso de conta de *e-mail* sendo usada para envio de *spam* (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.)
Solicitações	orçamento, documento, relatório, cotação de preços, lista de produtos

Tabela 2.1: Exemplos de tópicos e temas de mensagens de *phishing*.

Prevenção:

- fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em *links*;
- questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);
- fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
- não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada (mais detalhes na Seção 3.3 do Capítulo Ataques na Internet);
- seja cuidadoso ao acessar *links*. Procure digitar o endereço diretamente no navegador *Web*;
- verifique o *link* apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o *link* real para o *phishing*. Ao posicionar o *mouse* sobre o *link*, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
- utilize mecanismos de segurança, como programas *antimalware*, *firewall* pessoal e filtros *antiphishing* (mais detalhes no Capítulo Mecanismos de segurança);
- verifique se a página utiliza conexão segura. *Sites* de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados (mais detalhes na Seção 10.1.1 do Capítulo Uso seguro da Internet);
- verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao *site* verdadeiro (mais detalhes na Seção 10.1.2 do Capítulo Uso seguro da Internet);
- acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

2.3.1 *Pharming*

Pharming é um tipo específico de *phishing* que envolve a redireção da navegação do usuário para *sites* falsos, por meio de alterações no serviço de DNS (***D**omain **N**ame **S**ystem*). Neste caso, quando você tenta acessar um *site* legítimo, o seu navegador *Web* é redirecionado, de forma transparente, para uma página falsa. Esta redireção pode ocorrer:

- por meio do comprometimento do servidor de DNS do provedor que você utiliza;
- pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;

- pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou *modem* de banda larga.

Prevenção:

- desconfie se, ao digitar uma URL, for redirecionado para outro *site*, o qual tenta realizar alguma ação suspeita, como abrir um arquivo ou tentar instalar um programa;
- desconfie imediatamente caso o *site* de comércio eletrônico ou *Internet Banking* que você está acessando não utilize conexão segura. *Sites* confiáveis de comércio eletrônico e *Internet Banking* sempre usam conexões seguras quando dados pessoais e financeiros são solicitados (mais detalhes na Seção 10.1.1 do Capítulo Uso seguro da Internet);
- observe se o certificado apresentado corresponde ao do *site* verdadeiro (mais detalhes na Seção 10.1.2 do Capítulo Uso seguro da Internet).

2.4 Golpes de comércio eletrônico

Golpes de comércio eletrônico são aqueles nos quais golpistas, com o objetivo de obter vantagens financeiras, exploram a relação de confiança existente entre as partes envolvidas em uma transação comercial. Alguns destes golpes são apresentados nas próximas seções.

2.4.1 Golpe do *site* de comércio eletrônico fraudulento

Neste golpe, o golpista cria um *site* fraudulento, com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias.

Para aumentar as chances de sucesso, o golpista costuma utilizar artifícios como: enviar *spam*, fazer propaganda via *links* patrocinados, anunciar descontos em *sites* de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado.

Além do comprador, que paga mas não recebe a mercadoria, este tipo de golpe pode ter outras vítimas, como:

- uma empresa séria, cujo nome tenha sido vinculado ao golpe;
- um *site* de compras coletivas, caso ele tenha intermediado a compra;
- uma pessoa, cuja identidade tenha sido usada para a criação do *site* ou para abertura de empresas fantasmas.

Prevenção:

- faça uma pesquisa de mercado, comparando o preço do produto exposto no *site* com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;

- pesquise na Internet sobre o *site*, antes de efetuar a compra, para ver a opinião de outros clientes;
- acesse *sites* especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a esta empresa;
- fique atento a propagandas recebidas através de *spam* (mais detalhes no Capítulo *Spam*);
- seja cuidadoso ao acessar *links* patrocinados (mais detalhes na Seção 6.5 do Capítulo Outros riscos);
- procure validar os dados de cadastro da empresa no *site* da Receita Federal[4];
- não informe dados de pagamento caso o *site* não ofereça conexão segura ou não apresente um certificado confiável (mais detalhes na Seção 10.1 do Capítulo Uso seguro da Internet).

2.4.2 Golpe envolvendo *sites* de compras coletivas

Sites de compras coletivas têm sido muito usados em golpes de *sites* de comércio eletrônico fraudulentos, como descrito na Seção 2.4.1. Além dos riscos inerentes às relações comerciais cotidianas, os *sites* de compras coletivas também apresentam riscos próprios, gerados principalmente pela pressão imposta ao consumidor em tomar decisões rápidas pois, caso contrário, podem perder a oportunidade de compra.

Golpistas criam *sites* fraudulentos e os utilizam para anunciar produtos nos *sites* de compras coletivas e, assim, conseguir grande quantidade de vítimas em um curto intervalo de tempo.

Além disto, *sites* de compras coletivas também podem ser usados como tema de mensagens de *phishing*. Golpistas costumam mandar mensagens como se tivessem sido enviadas pelo *site* verdadeiro e, desta forma, tentam induzir o usuário a acessar uma página falsa e a fornecer dados pessoais, como número de cartão de crédito e senhas.

Prevenção:

- procure não comprar por impulso apenas para garantir o produto ofertado;
- seja cauteloso e faça pesquisas prévias, pois há casos de produtos anunciados com desconto, mas que na verdade, apresentam valores superiores aos de mercado;
- pesquise na Internet sobre o *site* de compras coletivas, antes de efetuar a compra, para ver a opinião de outros clientes e observar se foi satisfatória a forma como os possíveis problemas foram resolvidos;
- siga as dicas apresentadas na Seção 2.3 para se prevenir de golpes envolvendo *phishing*;
- siga as dicas apresentadas na Seção 2.4.1 para se prevenir de golpes envolvendo *sites* de comércio eletrônico fraudulento.

[4] `http://www.receita.fazenda.gov.br/`.

2.4.3 Golpe do *site* de leilão e venda de produtos

O golpe do *site* de leilão e venda de produtos é aquele, por meio do qual, um comprador ou vendedor age de má-fé e não cumpre com as obrigações acordadas ou utiliza os dados pessoais e financeiros envolvidos na transação comercial para outros fins. Por exemplo:

- o comprador tenta receber a mercadoria sem realizar o pagamento ou o realiza por meio de transferência efetuada de uma conta bancária ilegítima ou furtada;
- o vendedor tenta receber o pagamento sem efetuar a entrega da mercadoria ou a entrega danificada, falsificada, com características diferentes do anunciado ou adquirida de forma ilícita e criminosa (por exemplo, proveniente de contrabando ou de roubo de carga);
- o comprador ou o vendedor envia *e-mails* falsos, em nome do sistema de gerenciamento de pagamentos, como forma de comprovar a realização do pagamento ou o envio da mercadoria que, na realidade, não foi feito.

Prevenção:

- faça uma pesquisa de mercado, comparando o preço do produto com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;
- marque encontros em locais públicos caso a entrega dos produtos seja feita pessoalmente;
- acesse *sites* especializados em tratar reclamações de consumidores insatisfeitos e que os coloca em contato com os responsáveis pela venda (você pode avaliar se a forma como o problema foi resolvido foi satisfatória ou não);
- utilize sistemas de gerenciamento de pagamentos pois, além de dificultarem a aplicação dos golpes, impedem que seus dados pessoais e financeiros sejam enviados aos golpistas;
- procure confirmar a realização de um pagamento diretamente em sua conta bancária ou pelo *site* do sistema de gerenciamento de pagamentos (não confie apenas em *e-mails* recebidos, pois eles podem ser falsos);
- verifique a reputação do usuário[5] (muitos *sites* possuem sistemas que medem a reputação de compradores e vendedores, por meio da opinião de pessoas que já negociaram com este usuário);
- acesse os *sites*, tanto do sistema de gerenciamento de pagamentos como o responsável pelas vendas, diretamente do navegador, sem clicar em *links* recebidos em mensagens;
- mesmo que o vendedor lhe envie o código de rastreamento fornecido pelos Correios, não utilize esta informação para comprovar o envio e liberar o pagamento (até que você tenha a mercadoria em mãos não há nenhuma garantia de que o que foi enviado é realmente o que foi solicitado).

[5] As informações dos sistemas de reputação, apesar de auxiliarem na seleção de usuários, não devem ser usadas como única medida de prevenção, pois contas com reputação alta são bastante visadas para golpes de *phishing*.

2.5 Boato (*Hoax*)



Um boato, ou *hoax*, é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

Boatos podem trazer diversos problemas, tanto para aqueles que os recebem e os distribuem, como para aqueles que são citados em seus conteúdos. Entre estes diversos problemas, um boato pode:

- conter códigos maliciosos;
- espalhar desinformação pela Internet;
- ocupar, desnecessariamente, espaço nas caixas de *e-mails* dos usuários;
- comprometer a credibilidade e a reputação de pessoas ou entidades referenciadas na mensagem;
- comprometer a credibilidade e a reputação da pessoa que o repassa pois, ao fazer isto, esta pessoa estará supostamente endossando ou concordando com o conteúdo da mensagem;
- aumentar excessivamente a carga de servidores de *e-mail* e o consumo de banda de rede, necessários para a transmissão e o processamento das mensagens;
- indicar, no conteúdo da mensagem, ações a serem realizadas e que, se forem efetivadas, podem resultar em sérios danos, como apagar um arquivo que supostamente contém um código malicioso, mas que na verdade é parte importante do sistema operacional instalado no computador.

Prevenção:

Normalmente, os boatos se propagam pela boa vontade e solidariedade de quem os recebe, pois há uma grande tendência das pessoas em confiar no remetente, não verificar a procedência e não conferir a veracidade do conteúdo da mensagem. Para que você possa evitar a distribuição de boatos é muito importante conferir a procedência dos *e-mails* e, mesmo que tenham como remetente alguém conhecido, é preciso certificar-se de que a mensagem não é um boato.

Um boato, geralmente, apresenta pelo menos uma das seguintes características[6]:

- afirma não ser um boato;
- sugere consequências trágicas caso uma determinada tarefa não seja realizada;
- promete ganhos financeiros ou prêmios mediante a realização de alguma ação;
- apresenta erros gramaticais e de ortografia;
- apresenta informações contraditórias;

[6] Estas características devem ser usadas apenas como guia, pois podem existir boatos que não apresentem nenhuma delas, assim como podem haver mensagens legítimas que apresentem algumas.

- enfatiza que ele deve ser repassado rapidamente para o maior número de pessoas;
- já foi repassado diversas vezes (no corpo da mensagem, normalmente, é possível observar cabeçalhos de *e-mails* repassados por outras pessoas).

Além disto, muitas vezes, uma pesquisa na Internet pelo assunto da mensagem pode ser suficiente para localizar relatos e denúncias já feitas. É importante ressaltar que você **nunca** deve repassar boatos pois, ao fazer isto, estará endossando ou concordando com o seu conteúdo.

2.6 Prevenção

Outras dicas gerais para se proteger de golpes aplicados na Internet são:

Notifique: caso identifique uma tentativa de golpe, é importante notificar a instituição envolvida, para que ela possa tomar as providências que julgar cabíveis (mais detalhes na Seção 7.2 do Capítulo Mecanismos de segurança).

Mantenha-se informado: novas formas de golpes podem surgir, portanto é muito importante que você se mantenha informado. Algumas fontes de informação que você pode consultar são:

- seções de informática de jornais de grande circulação e de *sites* de notícias que, normalmente, trazem matérias ou avisos sobre os golpes mais recentes;
- *sites* de empresas mencionadas nas mensagens (algumas empresas colocam avisos em suas páginas quando percebem que o nome da instituição está sendo indevidamente usado);
- *sites* especializados que divulgam listas contendo os golpes que estão sendo aplicados e seus respectivos conteúdos. Alguns destes *sites* são:
  - Monitor das Fraudes
    `http://www.fraudes.org/` (em português)
  - Quatro Cantos
    `http://www.quatrocantos.com/LENDAS/` (em português)
  - *Snopes.com - Urban Legends Reference Pages*
    `http://www.snopes.com/` (em inglês)
  - *Symantec Security Response Hoaxes*
    `http://www.symantec.com/avcenter/hoax.html` (em inglês)
  - *TruthOrFiction.com*
    `http://www.truthorfiction.com/` (em inglês)
  - *Urban Legends and Folklore*
    `http://urbanlegends.about.com/` (em inglês)

3. Ataques na Internet



Ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque.

Os motivos que levam os atacantes a desferir ataques na Internet são bastante diversos, variando da simples diversão até a realização de ações criminosas. Alguns exemplos são:

Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.

Prestígio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.

Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes (mais detalhes no Capítulo Golpes na Internet).

Motivações ideológicas: tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.

Motivações comerciais: tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

Para alcançar estes objetivos os atacantes costumam usar técnicas, como as descritas nas próximas seções.

3.1 Exploração de vulnerabilidades

Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

3.2 Varredura em redes (*Scan*)

Varredura em redes, ou *scan*[1], é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

A varredura em redes e a exploração de vulnerabilidades associadas podem ser usadas de forma:

Legítima: por pessoas devidamente autorizadas, para verificar a segurança de computadores e redes e, assim, tomar medidas corretivas e preventivas.

Maliciosa: por atacantes, para explorar as vulnerabilidades encontradas nos serviços disponibilizados e nos programas instalados para a execução de atividades maliciosas. Os atacantes também podem utilizar os computadores ativos detectados como potenciais alvos no processo de propagação automática de códigos maliciosos e em ataques de força bruta (mais detalhes no Capítulo Códigos maliciosos (*Malware*) e na Seção 3.5, respectivamente).

3.3 Falsificação de *e-mail* (*E-mail spoofing*)

Falsificação de *e-mail*, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

[1]Não confunda *scan* com *scam*. *Scams*, com "m", são esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras (mais detalhes no Capítulo Golpes na Internet).

Esta técnica é possível devido a características do protocolo SMTP (***S**imple **M**ail **T**ransfer **P**rotocol*) que permitem que campos do cabeçalho, como "`From:`" (endereço de quem enviou a mensagem), "`Reply-To`" (endereço de resposta da mensagem) e "`Return-Path`" (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de *spam* e em golpes de *phishing*. Atacantes utilizam-se de endereços de *e-mail* coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.

Exemplos de *e-mails* com campos falsificados são aqueles recebidos como sendo:

- de alguém conhecido, solicitando que você clique em um *link* ou execute um arquivo anexo;
- do seu banco, solicitando que você siga um *link* fornecido na própria mensagem e informe dados da sua conta bancária;
- do administrador do serviço de *e-mail* que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie.

Você também pode já ter observado situações onde o seu próprio endereço de *e-mail* foi indevidamente utilizado. Alguns indícios disto são:

- você recebe respostas de *e-mails* que você nunca enviou;
- você recebe *e-mails* aparentemente enviados por você mesmo, sem que você tenha feito isto;
- você recebe mensagens de devolução de *e-mails* que você nunca enviou, reportando erros como usuário desconhecido e caixa de entrada lotada (cota excedida).

3.4 Interceptação de tráfego (*Sniffing*)

Interceptação de tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*. Esta técnica pode ser utilizada de forma:

Legítima: por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.

Maliciosa: por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Note que as informações capturadas por esta técnica são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las (mais detalhes no Capítulo Criptografia).

3.5 Força bruta (*Brute force*)

Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta. Dispositivos móveis, que estejam protegidos por senha, além de poderem ser atacados pela rede, também podem ser alvo deste tipo de ataque caso o atacante tenha acesso físico a eles.

Se um atacante tiver conhecimento do seu nome de usuário e da sua senha ele pode efetuar ações maliciosas em seu nome como, por exemplo:

- trocar a sua senha, dificultando que você acesse novamente o *site* ou computador invadido;
- invadir o serviço de *e-mail* que você utiliza e ter acesso ao conteúdo das suas mensagens e à sua lista de contatos, além de poder enviar mensagens em seu nome;
- acessar a sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;
- invadir o seu computador e, de acordo com as permissões do seu usuário, executar ações, como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.

Mesmo que o atacante não consiga descobrir a sua senha, você pode ter problemas ao acessar a sua conta caso ela tenha sofrido um ataque de força bruta, pois muitos sistemas bloqueiam as contas quando várias tentativas de acesso sem sucesso são realizadas.

Apesar dos ataques de força bruta poderem ser realizados manualmente, na grande maioria dos casos, eles são realizados com o uso de ferramentas automatizadas facilmente obtidas na Internet e que permitem tornar o ataque bem mais efetivo.

As tentativas de adivinhação costumam ser baseadas em:

- dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;
- substituições óbvias de caracteres, como trocar “`a`” por “`@`” e “`o`” por “`0`”;
- sequências numéricas e de teclado, como “`123456`”, “`qwert`” e “`1qaz2wsx`”;
- informações pessoais, de conhecimento prévio do atacante ou coletadas na Internet em redes sociais e *blogs*, como nome, sobrenome, datas e números de documentos.

Um ataque de força bruta, dependendo de como é realizado, pode resultar em um ataque de negação de serviço, devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo (mais detalhes no Capítulo Contas e senhas).

3.6 Desfiguração de página (*Defacement*)

Desfiguração de página, *defacement* ou pichação, é uma técnica que consiste em alterar o conteúdo da página *Web* de um *site*.

As principais formas que um atacante, neste caso também chamado de *defacer*, pode utilizar para desfigurar uma página *Web* são:

- explorar erros da aplicação *Web*;
- explorar vulnerabilidades do servidor de aplicação *Web*;
- explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação *Web*;
- invadir o servidor onde a aplicação *Web* está hospedada e alterar diretamente os arquivos que compõem o *site*;
- furtar senhas de acesso à interface *Web* usada para administração remota.

Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente, os atacantes alteram a página principal do *site*, porém páginas internas também podem ser alteradas.

3.7 Negação de serviço (DoS e DDoS)

Negação de serviço, ou DoS (***D**enial **o**f **S**ervice*), é uma técnica pela qual um atacante utiliza **um computador** para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando **um conjunto de computadores** é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (***D**istributed **D**enial **o**f **S**ervice*).

O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo. Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas.

Nos casos já registrados de ataques, os alvos ficaram impedidos de oferecer serviços durante o período em que eles ocorreram, mas, ao final, voltaram a operar normalmente, sem que tivesse havido vazamento de informações ou comprometimento de sistemas ou computadores.

Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de *botnets* (mais detalhes na Seção 4.3 do Capítulo Códigos maliciosos (*Malware*)).

Ataques de negação de serviço podem ser realizados por diversos meios, como:

- pelo envio de grande quantidade de requisições para um serviço, consumindo os recursos necessários ao seu funcionamento (processamento, número de conexões simultâneas, memória e espaço em disco, por exemplo) e impedindo que as requisições dos demais usuários sejam atendidas;

- pela geração de grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível qualquer acesso a computadores ou serviços desta rede;
- pela exploração de vulnerabilidades existentes em programas, que podem fazer com que um determinado serviço fique inacessível.

Nas situações onde há saturação de recursos, caso um serviço não tenha sido bem dimensionado, ele pode ficar inoperante ao tentar atender as próprias solicitações legítimas. Por exemplo, um *site* de transmissão dos jogos da Copa de Mundo pode não suportar uma grande quantidade de usuários que queiram assistir aos jogos finais e parar de funcionar.

3.8 Prevenção

O que define as chances de um ataque na Internet ser ou não bem sucedido é o conjunto de medidas preventivas tomadas pelos usuários, desenvolvedores de aplicações e administradores dos computadores, serviços e equipamentos envolvidos.

Se cada um fizer a sua parte, muitos dos ataques realizados via Internet podem ser evitados ou, ao menos, minimizados.

A parte que cabe a você, como usuário da Internet, é proteger os seus dados, fazer uso dos mecanismos de proteção disponíveis e manter o seu computador atualizado e livre de códigos maliciosos. Ao fazer isto, você estará contribuindo para a segurança geral da Internet, pois:

- quanto menor a quantidade de computadores vulneráveis e infectados, menor será a potência das *botnets* e menos eficazes serão os ataques de negação de serviço (mais detalhes na Seção 4.3, do Capítulo Códigos maliciosos (*Malware*));
- quanto mais consciente dos mecanismos de segurança você estiver, menores serão as chances de sucesso dos atacantes (mais detalhes no Capítulo Mecanismos de segurança);
- quanto melhores forem as suas senhas, menores serão as chances de sucesso de ataques de força bruta e, consequentemente, de suas contas serem invadidas (mais detalhes no Capítulo Contas e senhas);
- quanto mais os usuários usarem criptografia para proteger os dados armazenados nos computadores ou aqueles transmitidos pela Internet, menores serão as chances de tráfego em texto claro ser interceptado por atacantes (mais detalhes no Capítulo Criptografia);
- quanto menor a quantidade de vulnerabilidades existentes em seu computador, menores serão as chances de ele ser invadido ou infectado (mais detalhes no Capítulo Segurança de computadores).

Faça sua parte e contribua para a segurança da Internet, incluindo a sua própria!

4. Códigos maliciosos (*Malware*)



Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela auto-execução de mídias removíveis infectadas, como *pen-drives*;
- pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam* (mais detalhes nos Capítulos Golpes na Internet, Ataques na Internet e *Spam*, respectivamente).

Os principais tipos de códigos maliciosos existentes são apresentados nas próximas seções.

4.1 Vírus



Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de *e-mail*. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de *pen-drives*.

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:

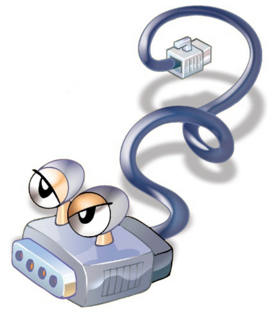
Vírus propagado por *e-mail*: recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no computador.

Vírus de *script*: escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página *Web* ou por *e-mail*, como um arquivo anexo ou como parte do próprio *e-mail* escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador *Web* e do programa leitor de *e-mails* do usuário.

Vírus de macro: tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).

Vírus de telefone celular: vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS (***M**ultimedia **M**essage **S**ervice*). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

4.2 *Worm*



Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

O processo de propagação e infecção dos *worms* ocorre da seguinte maneira:

a. **Identificação dos computadores alvos:** após infectar um computador, o *worm* tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras:

   - efetuar varredura na rede e identificar computadores ativos;
   - aguardar que outros computadores contatem o computador infectado;
   - utilizar listas, predefinidas ou obtidas na Internet, contendo a identificação dos alvos;
   - utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de *e-mail*.

b. **Envio das cópias:** após identificar os alvos, o *worm* efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:

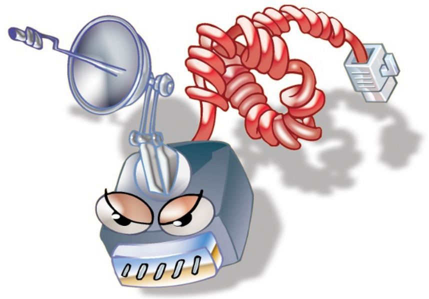
   - como parte da exploração de vulnerabilidades existentes em programas instalados no computador alvo;
   - anexadas a *e-mails*;
   - via canais de IRC (***I**nternet **R**elay **C**hat*);
   - via programas de troca de mensagens instantâneas;
   - incluídas em pastas compartilhadas em redes locais ou do tipo P2P (*Peer to Peer*).

c. **Ativação das cópias:** após realizado o envio da cópia, o *worm* necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

   - imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no computador alvo no momento do recebimento da cópia;
   - diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador;
   - pela realização de uma ação específica do usuário, a qual o *worm* está condicionado como, por exemplo, a inserção de uma mídia removível.

d. **Reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o computador que antes era o alvo passa a ser também o computador originador dos ataques.

4.3 *Bot* e *botnet*



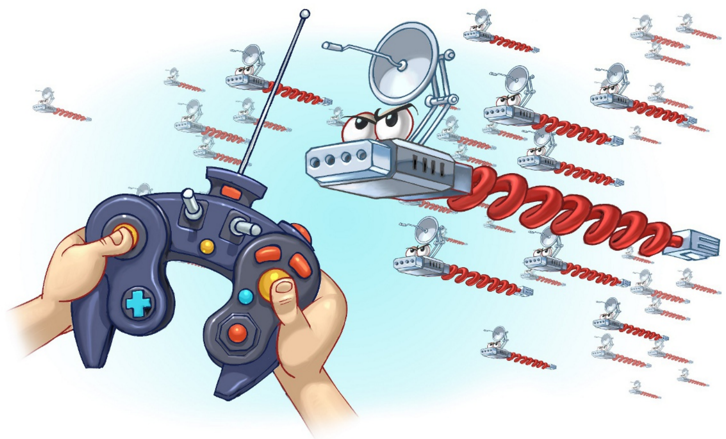
Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

A comunicação entre o invasor e o computador infectado pelo *bot* pode ocorrer via canais de IRC, servidores *Web* e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar *spam*.



Um computador infectado por um *bot* costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de *spam zombie* quando o *bot* instalado o transforma em um servidor de *e-mails* e o utiliza para o envio de *spam*.

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*.



Quanto mais zumbis participarem da *botnet* mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de *botnets* são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante (com o uso de *proxies* instalados nos zumbis).

O esquema simplificado apresentado a seguir exemplifica o funcionamento básico de uma *botnet*:

a. Um atacante propaga um tipo específico de *bot* na esperança de infectar e conseguir a maior quantidade possível de zumbis;

b. os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;

c. quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;

d. os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;

e. quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

4.4 *Spyware*



Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

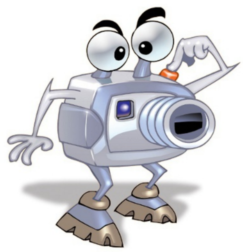
Legítimo: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

Malicioso: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas *spyware* são:



***Keylogger*:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*.



***Screenlogger*:** similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*.

***Adware*:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.



4.5 *Backdoor*



Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

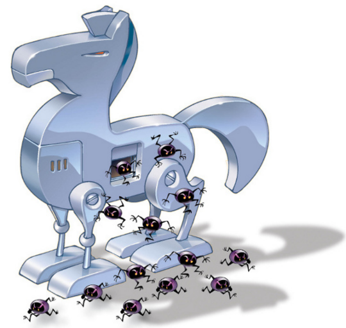
Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como *backdoors*.

Há casos de *backdoors* incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. Esses casos constituem uma séria ameaça à segurança de um computador que contenha um destes programas instalados pois, além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador.

4.6 Cavalo de troia (*Trojan*)



Cavalo de troia[1], *trojan* ou *trojan-horse*, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Exemplos de *trojans* são programas que você recebe ou obtém de *sites* na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.

Há diferentes tipos de *trojans*, classificados[2] de acordo com as ações maliciosas que costumam executar ao infectar um computador. Alguns destes tipos são:

[1] O "Cavalo de Troia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Troia.

[2] Esta classificação baseia-se em coletânea feita sobre os nomes mais comumente usados pelos programas *antimalware*.

***Trojan Downloader*:** instala outros códigos maliciosos, obtidos de *sites* na Internet.

***Trojan Dropper*:** instala outros códigos maliciosos, embutidos no próprio código do *trojan*.

***Trojan Backdoor*:** inclui *backdoors*, possibilitando o acesso remoto do atacante ao computador.

***Trojan DoS*:** instala ferramentas de negação de serviço e as utiliza para desferir ataques.

***Trojan* Destrutivo:** altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.

***Trojan Clicker*:** redireciona a navegação do usuário para *sites* específicos, com o objetivo de aumentar a quantidade de acessos a estes *sites* ou apresentar propagandas.

***Trojan Proxy*:** instala um servidor de *proxy*, possibilitando que o computador seja utilizado para navegação anônima e para envio de *spam*.

***Trojan Spy*:** instala programas *spyware* e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

***Trojan Banker* ou Bancos:** coleta dados bancários do usuário, através da instalação de programas *spyware* que são ativados quando *sites* de *Internet Banking* são acessados. É similar ao *Trojan Spy* porém com objetivos mais específicos.

4.7 *Rootkit*



Rootkit[3] é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

O conjunto de programas e técnicas fornecido pelos *rootkits* pode ser usado para:

- remover evidências em arquivos de *logs* (mais detalhes na Seção 7.6 do Capítulo Mecanismos de segurança);
- instalar outros códigos maliciosos, como *backdoors*, para assegurar o acesso futuro ao computador infectado;
- esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede, etc;
- mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede;
- capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego.

[3]O termo *rootkit* origina-se da junção das palavras "*root*" (que corresponde à conta de superusuário ou administrador do computador em sistemas Unix) e "*kit*" (que corresponde ao conjunto de programas usados para manter os privilégios de acesso desta conta).

É muito importante ressaltar que o nome *rootkit* não indica que os programas e as técnicas que o compõe são usadas para obter acesso privilegiado a um computador, mas sim para mantê-lo.

Rootkits inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os *rootkits* atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção.

Há casos de *rootkits* instalados propositalmente por empresas distribuidoras de CDs de música, sob a alegação de necessidade de proteção aos direitos autorais de suas obras. A instalação nestes casos costumava ocorrer de forma automática, no momento em que um dos CDs distribuídos contendo o código malicioso era inserido e executado. É importante ressaltar que estes casos constituem uma séria ameaça à segurança do computador, pois os *rootkits* instalados, além de comprometerem a privacidade do usuário, também podem ser reconfigurados e utilizados para esconder a presença e os arquivos inseridos por atacantes ou por outros códigos maliciosos.

4.8 Prevenção

Para manter o seu computador livre da ação dos códigos maliciosos existe um conjunto de medidas preventivas que você precisa adotar. Essas medidas incluem manter os programas instalados com as versões mais recentes e com todas as atualizações disponíveis aplicadas e usar mecanismos de segurança, como *antimalware* e *firewall* pessoal.

Além disso, há alguns cuidados que você e todos que usam o seu computador devem tomar sempre que forem manipular arquivos. Novos códigos maliciosos podem surgir, a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança.

Informações sobre os principais mecanismos de segurança que você deve utilizar são apresentados no Capítulo Mecanismos de segurança. Outros cuidados que você deve tomar para manter seu computador seguro são apresentados no Capítulo Segurança de computadores.

4.9 Resumo comparativo

Cada tipo de código malicioso possui características próprias que o define e o diferencia dos demais tipos, como forma de obtenção, forma de instalação, meios usados para propagação e ações maliciosas mais comuns executadas nos computadores infectados. Para facilitar a classificação e a conceituação, a Tabela 4.1 apresenta um resumo comparativo das características de cada tipo.

É importante ressaltar, entretanto, que definir e identificar essas características têm se tornado tarefas cada vez mais difíceis, devido às diferentes classificações existentes e ao surgimento de variantes que mesclam características dos demais códigos. Desta forma, o resumo apresentado na tabela não é definitivo e baseia-se nas definições apresentadas nesta Cartilha.

Códigos Maliciosos							
	Vírus	***Worm***	***Bot***	***Trojan***	***Spyware***	***Backdoor***	***Rootkit***
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópia de si próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Tabela 4.1: Resumo comparativo entre os códigos maliciosos.

5. *Spam*



Spam[1] é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (***U**nsolicited **C**ommercial **E**-mail*).

O *spam* em alguns pontos se assemelha a outras formas de propaganda, como a carta colocada na caixa de correio, o panfleto recebido na esquina e a ligação telefônica ofertando produtos. Porém, o que o difere é justamente o que o torna tão atraente e motivante para quem o envia (*spammer*): ao passo que nas demais formas o remetente precisa fazer algum tipo de investimento, o *spammer* necessita investir muito pouco, ou até mesmo nada, para alcançar os mesmos objetivos e em uma escala muito maior.

Desde o primeiro *spam* registrado e batizado como tal, em 1994, essa prática tem evoluído, acompanhando o desenvolvimento da Internet e de novas aplicações e tecnologias. Atualmente, o envio de *spam* é uma prática que causa preocupação, tanto pelo aumento desenfreado do volume de mensagens na rede, como pela natureza e pelos objetivos destas mensagens.

[1] Para mais detalhes acesse o *site* Antispam.br, `http://www.antispam.br/`, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), que constitui uma fonte de referência sobre o *spam* e tem o compromisso de informar usuários e administradores de redes sobre as implicações destas mensagens e as formas de proteção e de combate existentes.



Spams estão diretamente associados a ataques à segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

Algumas das formas como você pode ser afetado pelos problemas causados pelos *spams* são:

Perda de mensagens importantes: devido ao grande volume de *spam* recebido, você corre o risco de não ler mensagens importantes, lê-las com atraso ou apagá-las por engano.

Conteúdo impróprio ou ofensivo: como grande parte dos *spams* são enviados para conjuntos aleatórios de endereços de *e-mail*, é bastante provável que você receba mensagens cujo conteúdo considere impróprio ou ofensivo.

Gasto desnecessário de tempo: para cada *spam* recebido, é necessário que você gaste um tempo para lê-lo, identificá-lo e removê-lo da sua caixa postal, o que pode resultar em gasto desnecessário de tempo e em perda de produtividade.

Não recebimento de *e-mails*: caso o número de *spams* recebidos seja grande e você utilize um serviço de *e-mail* que limite o tamanho de caixa postal, você corre o risco de lotar a sua área de *e-mail* e, até que consiga liberar espaço, ficará impedido de receber novas mensagens.

Classificação errada de mensagens: caso utilize sistemas de filtragem com regras *antispam* ineficientes, você corre o risco de ter mensagens legítimas classificadas como *spam* e que, de acordo com as suas configurações, podem ser apagadas, movidas para quarentena ou redirecionadas para outras pastas de *e-mail*.



Independente do tipo de acesso à Internet usado, é o destinatário do *spam* quem paga pelo envio da mensagem. Os provedores, para tentar minimizar os problemas, provisionam mais recursos computacionais e os custos derivados acabam sendo transferidos e incorporados ao valor mensal que os usuários pagam.

Alguns dos problemas relacionados a *spam* que provedores e empresas costumam enfrentar são:

Impacto na banda: o volume de tráfego gerado pelos *spams* faz com que seja necessário aumentar a capacidade dos *links* de conexão com a Internet.

Má utilização dos servidores: boa parte dos recursos dos servidores de *e-mail*, como tempo de processamento e espaço em disco, são consumidos no tratamento de mensagens não solicitadas.

Inclusão em listas de bloqueio: um provedor que tenha usuários envolvidos em casos de envio de *spam* pode ter a rede incluída em listas de bloqueio, o que pode prejudicar o envio de *e-mails* por parte dos demais usuários e resultar em perda de clientes.

Investimento extra em recursos: os problemas gerados pelos *spams* fazem com que seja necessário aumentar os investimentos, para a aquisição de equipamentos e sistemas de filtragem e para a contratação de mais técnicos especializados na sua operação.

Os *spammers* utilizam diversas técnicas para coletar endereços de *e-mail*, desde a compra de bancos de dados até a produção de suas próprias listas, geradas a partir de:

Ataques de dicionário: consistem em formar endereços de *e-mail* a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.

Códigos maliciosos: muitos códigos maliciosos são projetados para varrer o computador infectado em busca de endereços de *e-mail* que, posteriormente, são repassados para os *spammers*.

***Harvesting*:** consiste em coletar endereços de *e-mail* por meio de varreduras em páginas *Web* e arquivos de listas de discussão, entre outros. Para tentar combater esta técnica, muitas páginas *Web* e listas de discussão apresentam os endereços de forma ofuscada (por exemplo, substituindo o "`@`" por "`(at)`" e os pontos pela palavra "`dot`"). Infelizmente, tais substituições são previstas por vários dos programas que implementam esta técnica.



Após efetuarem a coleta, os *spammers* procuram confirmar a existência dos endereços de *e-mail* e, para isto, costumam se utilizar de artifícios, como:

- enviar mensagens para os endereços coletados e, com base nas respostas recebidas dos servidores de *e-mail*, identificar quais endereços são válidos e quais não são;
- incluir no *spam* um suposto mecanismo para a remoção da lista de *e-mails*, como um *link* ou um endereço de *e-mail* (quando o usuário solicita a remoção, na verdade está confirmando para o *spammer* que aquele endereço de *e-mail* é válido e realmente utilizado);
- incluir no *spam* uma imagem do tipo *Web bug*, projetada para monitorar o acesso a uma página *Web* ou *e-mail* (quando o usuário abre o *spam*, o *Web bug* é acessado e o *spammer* recebe a confirmação que aquele endereço de *e-mail* é válido).

5.1 Prevenção



É muito importante que você saiba como identificar os *spams*, para poder detectá-los mais facilmente e agir adequadamente. As principais características[2] dos *spams* são:

Apresentam cabeçalho suspeito: o cabeçalho do *e-mail* aparece incompleto, por exemplo, os campos de remetente e/ou destinatário aparecem vazios ou com apelidos/nomes genéricos, como "`amigo@`" e "`suporte@`".

Apresentam no campo Assunto (*Subject*) palavras com grafia errada ou suspeita: a maioria dos filtros *antispam* utiliza o conteúdo deste campo para barrar *e-mails* com assuntos considerados suspeitos. No entanto, os *spammers* adaptam-se e tentam enganar os filtros colocando neste campo conteúdos enganosos, como ‘ ‘`vi@gra`" (em vez de "`viagra`").

[2] Vale ressaltar que nem todas essas características podem estar presentes ao mesmo tempo, em um mesmo *spam*. Da mesma forma, podem existir *spams* que não atendam às propriedades citadas, podendo, eventualmente, ser um novo tipo.

Apresentam no campo Assunto textos alarmantes ou vagos: na tentativa de confundir os filtros *antispam* e de atrair a atenção dos usuários, os *spammers* costumam colocar textos alarmantes, atraentes ou vagos demais, como "`Sua senha está inválida`", "`A informação que você pediu`" e "`Parabéns`".

Oferecem opção de remoção da lista de divulgação: alguns *spams* tentam justificar o abuso, alegando que é possível sair da lista de divulgação, clicando no endereço anexo ao *e-mail*. Este artifício, porém, além de não retirar o seu endereço de *e-mail* da lista, também serve para validar que ele realmente existe e que é lido por alguém.

Prometem que serão enviados "uma única vez": ao alegarem isto, sugerem que não é necessário que você tome alguma ação para impedir que a mensagem seja novamente enviada.

Baseiam-se em leis e regulamentações inexistentes: muitos *spams* tentam embasar o envio em leis e regulamentações brasileiras referentes à prática de *spam* que, até o momento de escrita desta Cartilha, não existem.

Alguns cuidados que você deve tomar para tentar reduzir a quantidade de *spams* recebidos são:

- procure filtrar as mensagens indesejadas, por meio de programas instalados em servidores ou em seu computador e de sistemas integrados a *Webmails* e leitores de *e-mails*. É interessante consultar o seu provedor de *e-mail*, ou o administrador de sua rede, para verificar os recursos existentes e como usá-los;
- alguns *Webmails* usam filtros baseados em "tira-teima", onde é exigido do remetente a confirmação do envio (após confirmá-la, ele é incluído em uma lista de remetentes autorizados e, a partir daí, pode enviar *e-mails* livremente). Ao usar esses sistemas, procure autorizar previamente os remetentes desejáveis, incluindo fóruns e listas de discussão, pois nem todos confirmam o envio e, assim, você pode deixar de receber mensagens importantes;
- muitos filtros colocam as mensagens classificadas como *spam* em quarentena. É importante que você, de tempos em tempos, verifique esta pasta, pois podem acontecer casos de falsos positivos e mensagens legítimas virem a ser classificadas como *spam*. Caso você, mesmo usando filtros, receba um *spam*, deve classificá-lo como tal, pois estará ajudando a treinar o filtro;
- seja cuidadoso ao fornecer seu endereço de *e-mail*. Existem situações onde não há motivo para que o seu *e-mail* seja fornecido. Ao preencher um cadastro, por exemplo, pense se é realmente necessário fornecer o seu *e-mail* e se você deseja receber mensagens deste local;
- fique atento a opções pré-selecionadas. Em alguns formulários ou cadastros preenchidos pela Internet, existe a pergunta se você quer receber *e-mails*, por exemplo, sobre promoções e lançamentos de produtos, cuja resposta já vem marcada como afirmativa. Fique atento a esta questão e desmarque-a, caso não deseje receber este tipo de mensagem;
- não siga *links* recebidos em *spams* e não responda mensagens deste tipo (estas ações podem servir para confirmar que seu *e-mail* é válido);
- desabilite a abertura de imagens em *e-mails* HTML (o fato de uma imagem ser acessada pode servir para confirmar que a mensagem foi lida);
- crie contas de *e-mail* secundárias e forneça-as em locais onde as chances de receber *spam* são grandes, como ao preencher cadastros em lojas e em listas de discussão;

- utilize as opções de privacidade das redes sociais (algumas redes permitem esconder o seu endereço de *e-mail* ou restringir as pessoas que terão acesso a ele);
- respeite o endereço de *e-mail* de outras pessoas. Use a opção de "`Bcc:`" ao enviar *e-mail* para grandes quantidades de pessoas. Ao encaminhar mensagens, apague a lista de antigos destinatários, pois mensagens reencaminhadas podem servir como fonte de coleta para *spammers*.

6. Outros riscos



Atualmente, devido à grande quantidade de serviços disponíveis, a maioria das ações dos usuários na Internet são executadas pelo acesso a páginas *Web*, seja pelo uso de navegadores ou de programas leitores de *e-mails* com capacidade de processar mensagens em formato HTML.

Para atender a grande demanda, incorporar maior funcionalidade e melhorar a aparência das páginas *Web*, novos recursos de navegação foram desenvolvidos e novos serviços foram disponibilizados. Estes novos recursos e serviços, infelizmente, não passaram despercebidos por pessoas mal-intencionadas, que viram neles novas possibilidades para coletar informações e aplicar golpes. Alguns destes recursos e serviços, os riscos que representam e os cuidados que você deve tomar ao utilizá-los são apresentados nas Seções 6.1, 6.2, 6.3, 6.4, 6.5 e 6.6.

Além disto, a grande quantidade de computadores conectados à rede propiciou e facilitou o compartilhamento de recursos entre os usuários, seja por meio de programas específicos ou pelo uso de opções oferecidas pelos próprios sistemas operacionais. Assim como no caso dos recursos e serviços *Web*, o compartilhamento de recursos também pode representar riscos e necessitar de alguns cuidados especiais, que são apresentados nas Seções 6.7 e 6.8.

6.1 *Cookies*

Cookies são pequenos arquivos que são gravados em seu computador quando você acessa *sites* na Internet e que são reenviados a estes mesmos *sites* quando novamente visitados. São usados para manter informações sobre você, como carrinho de compras, lista de produtos e preferências de navegação.

Um *cookie* pode ser temporário (de sessão), quando é apagado no momento em que o navegador *Web* ou programa leitor de *e-mail* é fechado, ou permanente (persistente), quando fica gravado no computador até expirar ou ser apagado. Também pode ser primário (*first-party*), quando definido pelo domínio do *site* visitado, ou de terceiros (*third-party*), quando pertencente a outro domínio (geralmente relacionado a anúncios ou imagens incorporados à página que está sendo visitada).

Alguns dos riscos relacionados ao uso de *cookies* são:

Compartilhamento de informações: as informações coletadas pelos *cookies* podem ser indevidamente compartilhadas com outros *sites* e afetar a sua privacidade. Não é incomum, por exemplo, acessar pela primeira vez um *site* de música e observar que as ofertas de CDs para o seu gênero musical preferido já estão disponíveis, sem que você tenha feito qualquer tipo de escolha.

Exploração de vulnerabilidades: quando você acessa uma página *Web*, o seu navegador disponibiliza uma série de informações sobre o seu computador, como *hardware*, sistema operacional e programas instalados. Os *cookies* podem ser utilizados para manter referências contendo estas informações e usá-las para explorar possíveis vulnerabilidades em seu computador.

Autenticação automática: ao usar opções como "Lembre-se de mim" e "Continuar conectado" nos *sites* visitados, informações sobre a sua conta de usuário são gravadas em *cookies* e usadas em autenticações futuras. Esta prática pode ser arriscada quando usada em computadores infectados ou de terceiros, pois os *cookies* podem ser coletados e permitirem que outras pessoas se autentiquem como você.

Coleta de informações pessoais: dados preenchidos por você em formulários *Web* também podem ser gravados em *cookies*, coletados por atacantes ou códigos maliciosos e indevidamente acessados, caso não estejam criptografados.

Coleta de hábitos de navegação: quando você acessa diferentes *sites* onde são usados *cookies* de terceiros, pertencentes a uma mesma empresa de publicidade, é possível a esta empresa determinar seus hábitos de navegação e, assim, comprometer a sua privacidade.

Prevenção:

Não é indicado bloquear totalmente o recebimento de *cookies*, pois isto pode impedir o uso adequado ou até mesmo o acesso a determinados *sites* e serviços. Para se prevenir dos riscos, mas sem comprometer a sua navegação, há algumas dicas que você deve seguir, como:

- ao usar um navegador *Web* baseado em níveis de permissão, como o Internet Explorer, procure não selecionar níveis de permissão inferiores a "médio";
- em outros navegadores ou programas leitores de *e-mail*, configure para que, por padrão, os *sites* não possam definir *cookies* e crie listas de exceções, cadastrando *sites* considerados confiáveis e onde o uso de *cookies* é realmente necessário, como *Webmails* e de *Internet Banking* e comércio eletrônico;

- caso você, mesmo ciente dos riscos, decida permitir que por padrão os *sites* possam definir *cookies*, procure criar uma lista de exceções e nela cadastre os *sites* que deseja bloquear;
- configure para que os *cookies* sejam apagados assim que o navegador for fechado;
- configure para não aceitar *cookies* de terceiros (ao fazer isto, a sua navegação não deverá ser prejudicada, pois apenas conteúdos relacionados a publicidade serão bloqueados);
- utilize opções de navegar anonimamente, quando usar computadores de terceiros (ao fazer isto, informações sobre a sua navegação, incluindo *cookies*, não serão gravadas).

Veja que, quando você altera uma configuração de privacidade ela é aplicada aos novos *cookies*, mas não aos que já estão gravados em seu computador. Assim, ao fazer isto, é importante que você remova os *cookies* já gravados para garantir que a nova configuração seja aplicada a todos.

6.2 Códigos móveis

Códigos móveis são utilizados por desenvolvedores para incorporar maior funcionalidade e melhorar a aparência de páginas *Web*. Embora sejam bastante úteis, podem representar riscos quando mal-implementados ou usados por pessoas mal-intencionadas.

Alguns tipos de códigos móveis e os riscos que podem representar são:

Programas e *applets Java*: normalmente os navegadores contêm módulos específicos para processar programas *Java* que, apesar de possuírem mecanismos de segurança, podem conter falhas de implementação e permitir que um programa Java hostil viole a segurança do computador.

***JavaScripts*:** assim como outros *scripts Web*, podem ser usados para causar violações de segurança em computadores. Um exemplo de ataque envolvendo *JavaScript* consiste em redirecionar usuários de um *site* legítimo para um *site* falso, para que instalem códigos maliciosos ou forneçam informações pessoais.

Componentes (ou controles) *ActiveX*: o navegador *Web*, pelo esquema de certificados digitais, verifica a procedência de um componente *ActiveX* antes de recebê-lo. Ao aceitar o certificado, o componente é executado e pode efetuar qualquer tipo de ação, desde enviar um arquivo pela Internet até instalar programas (que podem ter fins maliciosos) em seu computador (mais detalhes sobre certificados digitais são apresentados na Seção 9.4 do Capítulo Criptografia).

Prevenção:

Assim como no caso de *cookies*, não é indicado bloquear totalmente a execução dos códigos móveis, pois isto pode afetar o acesso a determinados *sites* e serviços. Para se prevenir dos riscos, mas sem comprometer a sua navegação, há algumas dicas que você deve seguir, como:

- permita a execução de programas *Java* e de *JavaScripts* mas assegure-se de utilizar complementos, como por exemplo o NoScript (disponível para alguns navegadores), para liberar gradualmente a execução, conforme necessário e apenas em *sites* confiáveis;

- permita que componentes *ActiveX* sejam executados em seu computador apenas quando vierem de *sites* conhecidos e confiáveis;
- seja cuidadoso ao permitir a instalação de componentes não assinados (mais detalhes na Seção 9.3 do Capítulo Criptografia).

6.3 Janelas de *pop-up*

Janelas de *pop-up* são aquelas que aparecem automaticamente e sem permissão, sobrepondo a janela do navegador *Web*, após você acessar um *site*. Alguns riscos que podem representar são:

- apresentar mensagens indesejadas, contendo propagandas ou conteúdo impróprio;
- apresentar *links*, que podem redirecionar a navegação para uma página falsa ou induzi-lo a instalar códigos maliciosos.

Prevenção:

- configure seu navegador *Web* para, por padrão, bloquear janelas de *pop-up*;
- crie uma lista de exceções, contendo apenas *sites* conhecidos e confiáveis e onde forem realmente necessárias.

6.4 *Plug-ins*, complementos e extensões

Plug-ins, complementos e extensões são programas geralmente desenvolvidos por terceiros e que você pode instalar em seu navegador *Web* ou leitor de *e-mails* para prover funcionalidades extras.

Esses programas, na maioria das vezes, são disponibilizados em repositórios, onde podem ser baixados livremente ou comprados. Alguns repositórios efetuam controle rígido sobre os programas antes de disponibilizá-los, outros utilizam classificações referentes ao tipo de revisão, enquanto outros não efetuam nenhum tipo de controle.

Apesar de grande parte destes programas serem confiáveis, há a chance de existir programas especificamente criados para executar atividades maliciosas ou que, devido a erros de implementação, possam executar ações danosas em seu computador.

Prevenção:

- assegure-se de ter mecanismos de segurança instalados e atualizados, antes de instalar programas desenvolvidos por terceiros (mais detalhes no Capítulo Mecanismos de segurança);
- mantenha os programas instalados sempre atualizados (mais detalhes no Capítulo Segurança de computadores);

- procure obter arquivos apenas de fontes confiáveis;
- utilize programas com grande quantidade de usuários (considerados populares) e que tenham sido bem avaliados. Muitos repositórios possuem sistema de classificação, baseado em quantidade de estrelas, concedidas de acordo com as avaliações recebidas. Selecione aqueles com mais estrelas;
- veja comentários de outros usuários sobre o programa, antes de instalá-lo (muitos *sites* disponibilizam listas de programas mais usados e mais recomendados);
- verifique se as permissões necessárias para a instalação e execução são coerentes, ou seja, um programa de jogos não necessariamente precisa ter acesso aos seus dados pessoais;
- seja cuidadoso ao instalar programas que ainda estejam em processo de revisão;
- denuncie aos responsáveis pelo repositório caso identifique programas maliciosos.

6.5 *Links* patrocinados

Um anunciante que queira fazer propaganda de um produto ou *site* paga para o *site* de busca apresentar o *link* em destaque quando palavras específicas são pesquisadas. Quando você clica em um *link* patrocinado, o *site* de busca recebe do anunciante um valor previamente combinado.

O anunciante geralmente possui uma página *Web* - com acesso via conta de usuário e senha - para interagir com o *site* de busca, alterar configurações, verificar acessos e fazer pagamentos. Este tipo de conta é bastante visado por atacantes, com o intuito de criar redirecionamentos para páginas de *phishing* ou contendo códigos maliciosos e representa o principal risco relacionado a *links* patrocinados.

Prevenção:

- não use *sites* de busca para acessar todo e qualquer tipo de *site*. Por exemplo: você não precisa pesquisar para saber qual é o *site* do seu banco, já que geralmente o endereço é bem conhecido.

6.6 *Banners* de propaganda

A Internet não trouxe novas oportunidades de negócio apenas para anunciantes e *sites* de busca. Usuários, de forma geral, podem obter rendimentos extras alugando espaço em suas páginas para serviços de publicidade.

Caso tenha uma página *Web*, você pode disponibilizar um espaço nela para que o serviço de publicidade apresente *banners* de seus clientes. Quanto mais a sua página é acessada e quanto mais cliques são feitos nos *banners* por intermédio dela, mais você pode vir a ser remunerado.

Infelizmente pessoas mal-intencionadas também viram no uso destes serviços novas oportunidades para aplicar golpes, denominados *malvertising*[1]. Este tipo de golpe consiste em criar anúncios

[1] *Malvertising* é uma palavra em inglês originada da junção de "*malicious*" (malicioso) e "*advertsing*" (propaganda).

maliciosos e, por meio de serviços de publicidade, apresentá-los em diversas páginas *Web*. Geralmente, o serviço de publicidade é induzido a acreditar que se trata de um anúncio legítimo e, ao aceitá-lo, intermedia a apresentação e faz com que ele seja mostrado em diversas páginas.

Prevenção:

- seja cuidadoso ao clicar em *banners* de propaganda (caso o anúncio lhe interesse, procure ir diretamente para a página do fabricante);
- mantenha o seu computador protegido, com as versões mais recentes e com todas as atualizações aplicadas (mais detalhes no Capítulo Segurança de computadores);
- utilize e mantenha atualizados mecanismos de segurança, como *antimalware* e *firewall* pessoal (mais detalhes no Capítulo Mecanismos de segurança);
- seja cuidadoso ao configurar as opções de privacidade em seu navegador *Web* (mais detalhes no Capítulo Privacidade).

6.7 Programas de distribuição de arquivos (P2P)

Programas de distribuição de arquivos, ou P2P, são aqueles que permitem que os usuários compartilhem arquivos entre si. Alguns exemplos são: Kazaa, Gnutella e BitTorrent. Alguns riscos relacionados ao uso destes programas são:

Acesso indevido: caso esteja mal configurado ou possua vulnerabilidades o programa de distribuição de arquivos pode permitir o acesso indevido a diretórios e arquivos (além dos compartilhados).

Obtenção de arquivos maliciosos: os arquivos distribuídos podem conter códigos maliciosos e assim, infectar seu computador ou permitir que ele seja invadido.

Violação de direitos autorais: a distribuição não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação desta lei.

Prevenção:

- mantenha seu programa de distribuição de arquivos sempre atualizado e bem configurado;
- certifique-se de ter um *antimalware* instalado e atualizado e o utilize para verificar qualquer arquivo obtido (mais detalhes no Capítulo Mecanismos de segurança);
- mantenha o seu computador protegido, com as versões mais recentes e com todas as atualizações aplicadas (mais detalhes no Capítulo Segurança de computadores);
- certifique-se que os arquivos obtidos ou distribuídos são livres, ou seja, não violam as leis de direitos autorais.

6.8 Compartilhamento de recursos

Alguns sistemas operacionais permitem que você compartilhe com outros usuários recursos do seu computador, como diretórios, discos, e impressoras. Ao fazer isto, você pode estar permitindo:

- o acesso não autorizado a recursos ou informações sensíveis;
- que seus recursos sejam usados por atacantes caso não sejam definidas senhas para controle de acesso ou sejam usadas senhas facilmente descobertas.

Por outro lado, assim como você pode compartilhar recursos do seu computador, você também pode acessar recursos que foram compartilhados por outros. Ao usar estes recursos, você pode estar se arriscando a abrir arquivos ou a executar programas que contenham códigos maliciosos.

Prevenção:

- estabeleça senhas para os compartilhamentos;
- estabeleça permissões de acesso adequadas, evitando que usuários do compartilhamento tenham mais acessos que o necessário;
- compartilhe seus recursos pelo tempo mínimo necessário;
- tenha um *antimalware* instalado em seu computador, mantenha-o atualizado e utilize-o para verificar qualquer arquivo compartilhado (mais detalhes no Capítulo Mecanismos de segurança);
- mantenha o seu computador protegido, com as versões mais recentes e com todas as atualizações aplicadas (mais detalhes no Capítulo Segurança de computadores).

7. Mecanismos de segurança



Agora que você já está ciente de alguns dos riscos relacionados ao uso de computadores e da Internet e que, apesar disso, reconhece que não é possível deixar de usar estes recursos, está no momento de aprender detalhadamente a se proteger.

No seu dia a dia, há cuidados que você toma, muitas vezes de forma instintiva, para detectar e evitar riscos. Por exemplo: o contato pessoal e a apresentação de documentos possibilitam que você confirme a identidade de alguém, a presença na agência do seu banco garante que há um relacionamento com ele, os Cartórios podem reconhecer a veracidade da assinatura de alguém, etc.

E como fazer isto na Internet, onde as ações são realizadas sem contato pessoal e por um meio de comunicação que, em princípio, é considerado inseguro?

Para permitir que você possa aplicar na Internet cuidados similares aos que costuma tomar em seu dia a dia, é necessário que os serviços disponibilizados e as comunicações realizadas por este meio garantam alguns requisitos básicos de segurança, como:

Identificação: permitir que uma entidade[1] se identifique, ou seja, diga quem ela é.

[1] Uma entidade pode ser, por exemplo, uma pessoa, uma empresa ou um programa de computador.

Autenticação: verificar se a entidade é realmente quem ela diz ser.

Autorização: determinar as ações que a entidade pode executar.

Integridade: proteger a informação contra alteração não autorizada.

Confidencialidade ou sigilo: proteger uma informação contra acesso não autorizado.

Não repúdio: evitar que uma entidade possa negar que foi ela quem executou uma ação.

Disponibilidade: garantir que um recurso esteja disponível sempre que necessário.

Para prover e garantir estes requisitos, foram adaptados e desenvolvidos os mecanismos de segurança que, quando corretamente configurados e utilizados, podem auxiliá-lo a se proteger dos riscos envolvendo o uso da Internet.

Antes de detalhar estes mecanismos, porém, é importante que você seja advertido sobre a possibilidade de ocorrência de **"falso positivo"**. Este termo é usado para designar uma situação na qual um mecanismo de segurança aponta uma atividade como sendo maliciosa ou anômala, quando na verdade trata-se de uma atividade legítima. Um falso positivo pode ser considerado um falso alarme (ou um alarme falso).

Um falso positivo ocorre, por exemplo, quando uma página legítima é classificada como *phishing*, uma mensagem legítima é considerada *spam*, um arquivo é erroneamente detectado como estando infectado ou um *firewall* indica como ataques algumas respostas dadas às solicitações feitas pelo próprio usuário.

Apesar de existir esta possibilidade, isto não deve ser motivo para que os mecanismos de segurança não sejam usados, pois a ocorrência destes casos é geralmente baixa e, muitas vezes, pode ser resolvida com alterações de configuração ou nas regras de verificação.

Nas próximas seções são apresentados alguns dos principais mecanismos de segurança e os cuidados que você deve tomar ao usar cada um deles.

7.1 Política de segurança

A política de segurança define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra.

É considerada como um importante mecanismo de segurança, tanto para as instituições como para os usuários, pois com ela é possível deixar claro o comportamento esperado de cada um. Desta forma, casos de mau comportamento, que estejam previstos na política, podem ser tratados de forma adequada pelas partes envolvidas.

A política de segurança pode conter outras políticas específicas, como:

Política de senhas: define as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca.

Política de *backup*: define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução.

Política de privacidade: define como são tratadas as informações pessoais, sejam elas de clientes, usuários ou funcionários.

Política de confidencialidade: define como são tratadas as informações institucionais, ou seja, se elas podem ser repassadas a terceiros.

Política de uso aceitável (PUA) ou *Acceptable Use Policy* (AUP): também chamada de "Termo de Uso" ou "Termo de Serviço", define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas.

A política de uso aceitável costuma ser disponibilizada na página *Web* e/ou ser apresentada no momento em que a pessoa passa a ter acesso aos recursos. Talvez você já tenha se deparado com estas políticas, por exemplo, ao ser admitido em uma empresa, ao contratar um provedor de acesso e ao utilizar serviços disponibilizados por meio da Internet, como redes sociais e *Webmail*.

Algumas situações que geralmente são consideradas de uso abusivo (não aceitável) são:

- compartilhamento de senhas;
- divulgação de informações confidenciais;
- envio de boatos e mensagens contendo *spam* e códigos maliciosos;
- envio de mensagens com objetivo de difamar, caluniar ou ameaçar alguém;
- cópia e distribuição não autorizada de material protegido por direitos autorais;
- ataques a outros computadores;
- comprometimento de computadores ou redes.

O desrespeito à política de segurança ou à política de uso aceitável de uma instituição pode ser considerado como um incidente de segurança e, dependendo das circunstâncias, ser motivo para encerramento de contrato (de trabalho, de prestação de serviços, etc.).

Cuidados a serem tomados:

- procure estar ciente da política de segurança da empresa onde você trabalha e dos serviços que você utiliza (como *Webmail* e redes sociais);
- fique atento às mudanças que possam ocorrer nas políticas de uso e de privacidade dos serviços que você utiliza, principalmente aquelas relacionadas ao tratamento de dados pessoais, para não ser surpreendido com alterações que possam comprometer a sua privacidade;
- fique atento à política de confidencialidade da empresa onde você trabalha e seja cuidadoso ao divulgar informações profissionais, principalmente em *blogs* e redes sociais (mais detalhes na Seção 11.1 do Capítulo Privacidade);
- notifique sempre que se deparar com uma atitude considerada abusiva (mais detalhes na Seção 7.2).

7.2 Notificação de incidentes e abusos

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Alguns exemplos de incidentes de segurança são: tentativa de uso ou acesso não autorizado a sistemas ou dados, tentativa de tornar serviços indisponíveis, modificação em sistemas (sem o conhecimento ou consentimento prévio dos donos) e o desrespeito à política de segurança ou à política de uso aceitável de uma instituição.

É muito importante que você notifique sempre que se deparar com uma atitude que considere abusiva ou com um incidente de segurança. De modo geral, a lista de pessoas/entidades a serem notificadas inclui: os responsáveis pelo computador que originou a atividade, os responsáveis pela rede que originou o incidente (incluindo o grupo de segurança e abusos, se existir um para aquela rede) e o grupo de segurança e abusos da rede a qual você está conectado (seja um provedor, empresa, universidade ou outro tipo de instituição).

Ao notificar um incidente, além de se proteger e contribuir para a segurança global da Internet, também ajudará outras pessoas a detectarem problemas, como computadores infectados, falhas de configuração e violações em políticas de segurança ou de uso aceitável de recursos.

Para encontrar os responsáveis por uma rede você deve consultar um "servidor de WHOIS", onde são mantidas as bases de dados sobre os responsáveis por cada bloco de números IP existentes. Para IPs alocados ao Brasil você pode consultar o servidor em `http://registro.br/cgi-bin/whois/`, para os demais países você pode acessar o *site* `http://www.geektools.com/whois.php` que aceita consultas referentes a qualquer número IP e as redireciona para os servidores apropriados[2].

É importante que você mantenha o CERT.br na cópia das suas notificações[3], pois isto contribuirá para as atividades deste grupo e permitirá que:

- os dados relativos a vários incidentes sejam correlacionados, ataques coordenados sejam identificados e novos tipos de ataques sejam descobertos;
- ações corretivas possam ser organizadas em cooperação com outras instituições;
- sejam geradas estatísticas que reflitam os incidentes ocorridos na Internet brasileira;
- sejam geradas estatísticas sobre a incidência e origem de *spams* no Brasil;
- sejam escritos documentos, como recomendações e manuais, direcionados às necessidades dos usuários da Internet no Brasil.

A notificação deve incluir a maior quantidade de informações possível, tais como:

- *logs* completos;
- data, horário e fuso horário (*time zone*) dos *logs* ou da atividade que está sendo notificada;

[2]Os *e-mails* encontrados nestas consultas não são necessariamente da pessoa que praticou o ataque, mas sim dos responsáveis pela rede à qual o computador está conectado, ou seja, podem ser os administradores da rede, sócios da empresa, ou qualquer outra pessoa que foi designada para cuidar da conexão da instituição com a Internet.

[3]Os endereços de *e-mail* usados pelo CERT.br para o tratamento de incidentes de segurança são: `cert@cert.br` (para notificações gerais) e `mail-abuse@cert.br` (específico para reclamações de *spam*).

- o *e-mail* completo, incluindo cabeçalhos e conteúdo (no caso de notificação de *spam*, *trojan*, *phishing* ou outras atividades maliciosas recebidas por *e-mail*);
- dados completos do incidente ou qualquer outra informação que tenha sido utilizada para identificar a atividade.

Outras informações e respostas para as dúvidas mais comuns referentes ao processo de notificação de incidentes podem ser encontradas na lista de questões mais frequentes (FAQ) mantida pelo CERT.br e disponível em `http://www.cert.br/docs/faq1.html`.

7.3 Contas e senhas

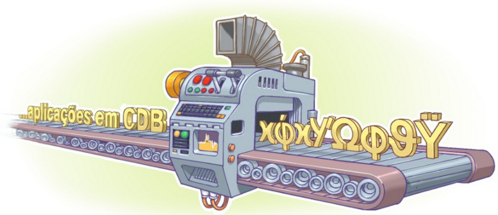


Contas e senhas são atualmente o mecanismo de autenticação mais usado para o controle de acesso a *sites* e serviços oferecidos pela Internet.

É por meio das suas contas e senhas que os sistemas conseguem saber quem você é e definir as ações que você pode realizar.

Dicas de elaboração, alteração e gerenciamento, assim como os cuidados que você deve ter ao usar suas contas e senhas, são apresentados no Capítulo Contas e senhas.

7.4 Criptografia



Usando criptografia você pode proteger seus dados contra acessos indevidos, tanto os que trafegam pela Internet como os já gravados em seu computador.

Detalhes sobre como a criptografia pode contribuir para manter a segurança dos seus dados e os conceitos de certificados e assinaturas digitais são apresentados no Capítulo Criptografia.

Detalhes sobre como a criptografia pode ser usada para garantir a conexão segura aos *sites* na Internet são apresentados na Seção 10.1 do Capítulo Uso seguro da Internet.

7.5 Cópias de segurança (*Backups*)

Você já imaginou o que aconteceria se, de uma hora para outra, perdesse alguns ou até mesmo todos os dados armazenados em seu computador? E se fossem todas as suas fotos ou os dados armazenados em seus dispositivos móveis? E se, ao enviar seu computador para manutenção, você o recebesse de volta com o disco rígido formatado? Para evitar que estas situações aconteçam, é necessário que você aja de forma preventiva e realize cópias de segurança (*backups*).

Muitas pessoas, infelizmente, só percebem a importância de ter *backups* quando já é tarde demais, ou seja, quando os dados já foram perdidos e não se pode fazer mais nada para recuperá-los. *Backups* são extremamente importantes, pois permitem:

Proteção de dados: você pode preservar seus dados para que sejam recuperados em situações como falha de disco rígido, atualização mal-sucedida do sistema operacional, exclusão ou substituição acidental de arquivos, ação de códigos maliciosos/atacantes e furto/perda de dispositivos.

Recuperação de versões: você pode recuperar uma versão antiga de um arquivo alterado, como uma parte excluída de um texto editado ou a imagem original de uma foto manipulada.

Arquivamento: você pode copiar ou mover dados que deseja ou que precisa guardar, mas que não são necessários no seu dia a dia e que raramente são alterados.

Muitos sistemas operacionais já possuem ferramentas de *backup* e recuperação integradas e também há a opção de instalar programas externos. Na maioria dos casos, ao usar estas ferramentas, basta que você tome algumas decisões, como:

Onde gravar os *backups*: você pode usar mídias (como CD, DVD, *pen-drive*, disco de Blu-ray e disco rígido interno ou externo) ou armazená-los remotamente (*online* ou *off-site*). A escolha depende do programa de *backup* que está sendo usado e de questões como capacidade de armazenamento, custo e confiabilidade. Um CD, DVD ou Blu-ray pode bastar para pequenas quantidades de dados, um *pen-drive* pode ser indicado para dados constantemente modificados, ao passo que um disco rígido pode ser usado para grandes volumes que devam perdurar.

Quais arquivos copiar: apenas arquivos confiáveis[4] e que tenham importância para você devem ser copiados. Arquivos de programas que podem ser reinstalados, geralmente, não precisam ser copiados. Fazer cópia de arquivos desnecessários pode ocupar espaço inutilmente e dificultar a localização dos demais dados. Muitos programas de *backup* já possuem listas de arquivos e diretórios recomendados, você pode optar por aceitá-las ou criar suas próprias listas.

Com que periodicidade devo realizá-los: depende da frequência com que você cria ou modifica arquivos. Arquivos frequentemente modificados podem ser copiados diariamente ao passo que aqueles pouco alterados podem ser copiados semanalmente ou mensalmente.

Cuidados a serem tomados:

- mantenha seus *backups* atualizados, de acordo com a frequência de alteração dos dados;
- mantenha seus *backups* em locais seguros, bem condicionados (longe de poeira, muito calor ou umidade) e com acesso restrito (apenas de pessoas autorizadas);
- configure para que seus *backups* sejam realizados automaticamente e certifique-se de que eles estejam realmente sendo feitos (*backups* manuais estão mais propensos a erros e esquecimento);
- além dos *backups* periódicos, sempre faça *backups* antes de efetuar grandes alterações no sistema (adição de *hardware*, atualização do sistema operacional, etc.) e de enviar o computador para manutenção;
- armazene dados sensíveis em formato criptografado (mais detalhes no Capítulo Criptografia);

[4] Arquivos que possam conter códigos maliciosos ou ter sido modificados/substituídos por invasores não devem ser copiados.

- mantenha *backups* redundantes, ou seja, várias cópias, para evitar perder seus dados em um incêndio, inundação, furto ou pelo uso de mídias defeituosas (você pode escolher pelo menos duas das seguintes possibilidades: sua casa, seu escritório e um repositório remoto);
- cuidado com mídias obsoletas (disquetes já foram muito usados para *backups*, porém, atualmente, acessá-los têm-se se tornado cada vez mais complicado pela dificuldade em encontrar computadores com leitores deste tipo de mídia e pela degradação natural do material);
- assegure-se de conseguir recuperar seus *backups* (a realização de testes periódicos pode evitar a péssima surpresa de descobrir que os dados estão corrompidos, em formato obsoleto ou que você não possui mais o programa de recuperação);
- mantenha seus *backups* organizados e identificados (você pode etiquetá-los ou nomeá-los com informações que facilitem a localização, como tipo do dado armazenado e data de gravação);
- copie dados que você considere importantes e evite aqueles que podem ser obtidos de fontes externas confiáveis, como os referentes ao sistema operacional ou aos programas instalados;
- nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis.

Ao utilizar serviços de *backup online* há alguns cuidados adicionais que você deve tomar, como:

- observe a disponibilidade do serviço e procure escolher um com poucas interrupções (alta disponibilidade);
- observe o tempo estimado de transmissão de dados (tanto para realização do *backup* quanto para recuperação dos dados). Dependendo da banda disponível e da quantidade de dados a ser copiada (ou recuperada), o *backup online* pode se tornar impraticável;
- seja seletivo ao escolher o serviço. Observe critérios como suporte, tempo no mercado (há quanto tempo o serviço é oferecido), a opinião dos demais usuários e outras referências que você possa ter;
- leve em consideração o tempo que seus arquivos são mantidos, o espaço de armazenagem e a política de privacidade e de segurança;
- procure aqueles nos quais seus dados trafeguem pela rede de forma criptografada (caso não haja esta possibilidade, procure você mesmo criptografar os dados antes de enviá-los).

7.6 Registro de eventos (*Logs*)

Log[5] é o registro de atividade gerado por programas e serviços de um computador. Ele pode ficar armazenado em arquivos, na memória do computador ou em bases de dados. A partir da análise desta informação você pode ser capaz de:

[5] *Log* é um termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo, de conexão (informações sobre a conexão de um computador à Internet) e de acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet). Na Cartilha este termo é usado para se referir ao registro das atividades que ocorrem no computador do usuário.

- detectar o uso indevido do seu computador, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema;
- detectar um ataque, como de força bruta ou a exploração de alguma vulnerabilidade;
- rastrear (auditar) as ações executadas por um usuário no seu computador, como programas utilizados, comandos executados e tempo de uso do sistema;
- detectar problemas de *hardware* ou nos programas e serviços instalados no computador.

Baseado nisto, você pode tomar medidas preventivas para tentar evitar que um problema maior ocorra ou, caso não seja possível, tentar reduzir os danos. Alguns exemplos são:

- se o disco rígido do seu computador estiver apresentando mensagens de erro, você pode se antecipar, fazer *backup* dos dados nele contidos e no momento oportuno enviá-lo para manutenção;
- se um atacante estiver tentando explorar uma vulnerabilidade em seu computador, você pode verificar se as medidas preventivas já foram aplicadas e tentar evitar que o ataque ocorra;
- se não for possível evitar um ataque, os *logs* podem permitir que as ações executadas pelo atacante sejam rastreadas, como arquivos alterados e as informações acessadas.

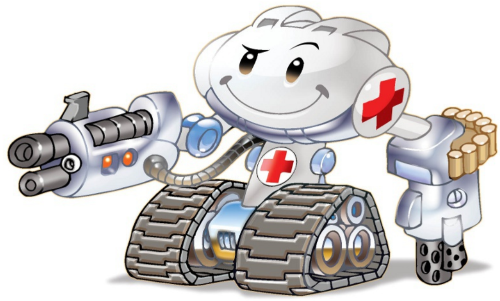
Logs são essenciais para notificação de incidentes, pois permitem que diversas informações importantes sejam detectadas, como por exemplo: a data e o horário em que uma determinada atividade ocorreu, o fuso horário do *log*, o endereço IP de origem da atividade, as portas envolvidas e o protocolo utilizado no ataque (TCP, UDP, ICMP, etc.), os dados completos que foram enviados para o computador ou rede e o resultado da atividade (se ela ocorreu com sucesso ou não).

Cuidados a serem tomados:

- mantenha o seu computador com o horário correto (o horário em que o *log* é registrado é usado na correlação de incidentes de segurança e, por este motivo, deve estar sincronizado[6]);
- verifique o espaço em disco livre em seu computador (*logs* podem ocupar bastante espaço em disco, dependendo das configurações feitas);
- evite registrar dados desnecessários, pois isto, além de poder ocupar espaço excessivo no disco, também pode degradar o desempenho do computador, comprometer a execução de tarefas básicas e dificultar a localização de informações de interesse;
- fique atento e desconfie caso perceba que os *logs* do seu computador foram apagados ou que deixaram de ser gerados por um período (muitos atacantes, na tentativa de esconder as ações executadas, desabilitam os serviços de *logs* e apagam os registros relacionados ao ataque ou, até mesmo, os próprios arquivos de *logs*);
- restrinja o acesso aos arquivos de *logs*. Não é necessário que todos os usuários tenham acesso às informações contidas nos *logs*. Por isto, sempre que possível, permita que apenas o usuário administrador tenha acesso a estes dados.

[6]Informações sobre como manter o horário do seu computador sincronizado podem ser obtidas em http://ntp.br/.

7.7 Ferramentas *antimalware*



Ferramentas *antimalware* são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, *antispyware*, *antirootkit* e *antitrojan* são exemplos de ferramentas deste tipo.

Ainda que existam ferramentas específicas para os diferentes tipos de códigos maliciosos, muitas vezes é difícil delimitar a área de atuação de cada uma delas, pois a definição do tipo de código malicioso depende de cada fabricante e muitos códigos mesclam as características dos demais tipos (mais detalhes no Capítulo Códigos maliciosos (*Malware*)).

Entre as diferentes ferramentas existentes, a que engloba a maior quantidade de funcionalidades é o antivírus. Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso.

Há diversos tipos de programas *antimalware* que diferem entre si das seguintes formas:

Método de detecção: assinatura (uma lista de assinaturas[7] é usada à procura de padrões), heurística (baseia-se nas estruturas, instruções e características que o código malicioso possui) e comportamento (baseia-se no comportamento apresentado pelo código malicioso quando executado) são alguns dos métodos mais comuns.

Forma de obtenção: podem ser gratuitos (quando livremente obtidos na Internet e usados por prazo indeterminado), experimentais (*trial*, usados livremente por um prazo predeterminado) e pagos (exigem que uma licença seja adquirida). Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras, além de poder contar com suporte.

Execução: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador *Web*. Também podem ser *online*, quando enviados para serem executados em servidores remotos, por um ou mais programas.

Funcionalidades apresentadas: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidade integradas, como a possibilidade de geração de discos de emergência e *firewall* pessoal (mais detalhes na Seção 7.8).

Alguns exemplos de *antimalware online* são:

- Anubis - *Analyzing Unknown Binaries*
  http://anubis.iseclab.org/
- Norman Sandbox - *SandBox Information Center*
  http://www.norman.com/security_center/security_tools/
- ThreatExpert - *Automated Threat Analysis*
  http://www.threatexpert.com/

[7] A assinatura de um código malicioso corresponde a características específicas nele contidas e que permitem que seja identificado unicamente. Um arquivo de assinaturas corresponde ao conjunto de assinaturas definidas pelo fabricante para os códigos maliciosos já detectados.

- VirusTotal - *Free Online Virus, Malware and URL Scanner*
  https://www.virustotal.com/

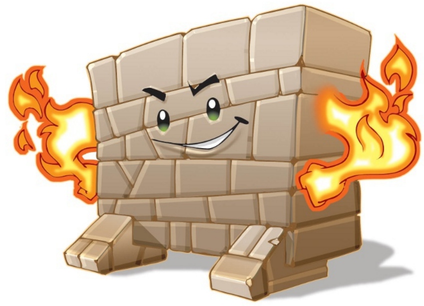
Para escolher o *antimalware* que melhor se adapta à sua necessidade é importante levar em conta o uso que você faz e as características de cada versão. Observe que não há relação entre o custo e a eficiência de um programa, pois há versões gratuitas que apresentam mais funcionalidades que versões pagas de outros fabricantes. Alguns *sites* apresentam comparativos entre os programas de diferentes fabricantes que podem guiá-lo na escolha do qual melhor lhe atende, tais como:

- AV-Comparatives - *Independent Tests of Anti-Virus Software*
  http://www.av-comparatives.org/
- Virus Bulletin - *Independent Malware Advice*
  http://www.virusbtn.com/

Cuidados a serem tomados:

- tenha um *antimalware* instalado em seu computador (programas *online*, apesar de bastante úteis, exigem que seu computador esteja conectado à Internet para que funcionem corretamente e podem conter funcionalidades reduzidas);
- utilize programas *online* quando suspeitar que o *antimalware* local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião (quiser confirmar o estado de um arquivo que já foi verificado pelo *antimalware* local);
- configure o *antimalware* para verificar toda e qualquer extensão de arquivo;
- configure o *antimalware* para verificar automaticamente arquivos anexados aos *e-mails* e obtidos pela Internet;
- configure o *antimalware* para verificar automaticamente os discos rígidos e as unidades removíveis (como *pen-drives*, CDs, DVDs e discos externos);
- mantenha o arquivo de assinaturas sempre atualizado (configure o *antimalware* para atualizá-lo automaticamente pela rede, de preferência diariamente);
- mantenha o *antimalware* sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas;
- evite executar simultaneamente diferentes programas *antimalware* (eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro);
- crie um disco de emergência e o utilize-o quando desconfiar que o *antimalware* instalado está desabilitado/comprometido ou que o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência, etc.).

7.8 *Firewall* pessoal



Firewall pessoal é um tipo específico de *firewall* que é utilizado para proteger um computador contra acessos não autorizados vindos da Internet.

Os programas *antimalware*, apesar da grande quantidade de funcionalidades, não são capazes de impedir que um atacante tente explorar, via rede, alguma vulnerabilidade existente em seu computador e nem de evitar o acesso não autorizado, caso haja algum *backdoor* nele instalado[8]. Devido a isto, além da instalação do *antimalware*, é necessário que você utilize um *firewall* pessoal.

Quando bem configurado, o *firewall* pessoal pode ser capaz de:

- registrar as tentativas de acesso aos serviços habilitados no seu computador;
- bloquear o envio para terceiros de informações coletadas por invasores e códigos maliciosos;
- bloquear as tentativas de invasão e de exploração de vulnerabilidades do seu computador e possibilitar a identificação das origens destas tentativas;
- analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado;
- evitar que um código malicioso já instalado seja capaz de se propagar, impedindo que vulnerabilidades em outros computadores sejam exploradas.

Alguns sistemas operacionais possuem *firewall* pessoal integrado. Caso o sistema instalado em seu computador não possua um ou você não queira usá-lo, há diversas opções disponíveis (pagas ou gratuitas). Você também pode optar por um *antimalware* com funcionalidades de *firewall* pessoal integradas.

Cuidados a serem tomados:

- antes de obter um *firewall* pessoal, verifique a procedência e certifique-se de que o fabricante é confiável;
- certifique-se de que o *firewall* instalado esteja ativo (estado: ativado);
- configure seu *firewall* para registrar a maior quantidade de informações possíveis (desta forma, é possível detectar tentativas de invasão ou rastrear as conexões de um invasor).

As configurações do *firewall* dependem de cada fabricante. De forma geral, a mais indicada é:

- liberar todo tráfego de saída do seu computador (ou seja, permitir que seu computador acesse outros computadores e serviços) e;
- bloquear todo tráfego de entrada ao seu computador (ou seja, impedir que seu computador seja acessado por outros computadores e serviços) e liberar as conexões conforme necessário, de acordo com os programas usados.

[8] Exceto aqueles que possuem *firewall* pessoal integrado.

7.9 Filtro *antispam*



Os filtros *antispam* já vem integrado à maioria dos *Webmails* e programas leitores de *e-mails* e permite separar os *e-mails* desejados dos indesejados (*spams*). A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas *spam* e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens.

Mais informações sobre filtros *antispam* e cuidados a serem tomados podem ser encontradas em http://antispam.br/. Mais detalhes sobre outras formas de prevenção contra *spam* são apresentadas no Capítulo *Spam*.

7.10 Outros mecanismos

Filtro *antiphishing*: já vem integrado à maioria dos navegadores *Web* e serve para alertar os usuários quando uma página suspeita de ser falsa é acessada. O usuário pode então decidir se quer acessá-la mesmo assim ou navegar para outra página.

Filtro de janelas de *pop-up*: já vem integrado à maioria dos navegadores *Web* e permite que você controle a exibição de janelas de *pop-up*. Você pode optar por bloquear, liberar totalmente ou permitir apenas para *sites* específicos.

Filtro de códigos móveis: filtros, como o NoScript, permitem que você controle a execução de códigos *Java* e *JavaScript*. Você pode decidir quando permitir a execução destes códigos e se eles serão executados temporariamente ou permanentemente - http://noscript.net/

Filtro de bloqueio de propagandas: filtros, como o Adblock, permitem o bloqueio de *sites* conhecidos por apresentarem propagandas - http://adblockplus.org/

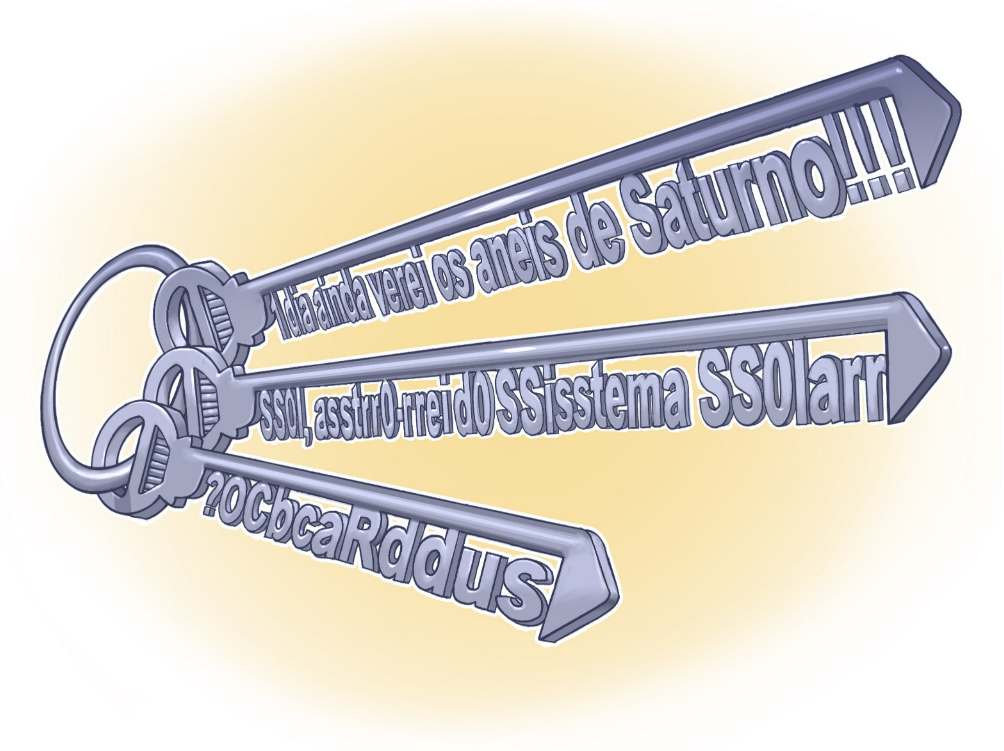
Teste de reputação de *site*: complementos, como o WOT (*Web of Trust*), permitem determinar a reputação dos *sites* que você acessa. Por meio de um esquema de cores, ele indica a reputação do *site*, como: verde escuro (excelente), verde claro (boa), amarelo (insatisfatória), vermelho claro (má) e vermelho escuro (péssima) - http://www.mywot.com/

Programa para verificação de vulnerabilidades: programas, como o PSI (*Secunia Personal Software Inspector*), permitem verificar vulnerabilidades nos programas instalados em seu computador e determinar quais devem ser atualizados -
http://secunia.com/vulnerability_scanning/personal/

***Sites* e complementos para expansão de *links* curtos:** complementos ou *sites* específicos, como o LongURL, permitem verificar qual é o *link* de destino de um *link* curto. Desta forma, você pode verificar a URL de destino, sem que para isto necessite acessar o *link* curto -
http://longurl.org/

***Anonymizer*:** *sites* para navegação anônima, conhecidos como *anonymizers*, intermediam o envio e recebimento de informações entre o seu navegador *Web* e o *site* que você deseja visitar. Desta forma, o seu navegador não recebe *cookies* e as informações por ele fornecidas não são repassadas para o *site* visitado - http://www.anonymizer.com/

8. Contas e senhas



Uma conta de usuário, também chamada de “nome de usuário”, “nome de *login*” e *username*, corresponde à identificação única de um usuário em um computador ou serviço. Por meio das contas de usuário é possível que um mesmo computador ou serviço seja compartilhado por diversas pessoas, pois permite, por exemplo, identificar unicamente cada usuário, separar as configurações específicas de cada um e controlar as permissões de acesso.

A sua conta de usuário é de conhecimento geral e é o que permite a sua identificação. Ela é, muitas vezes, derivada do seu próprio nome, mas pode ser qualquer sequência de caracteres que permita que você seja identificado unicamente, como o seu endereço de *e-mail*. Para garantir que ela seja usada apenas por você, e por mais ninguém, é que existem os mecanismos de autenticação.

Existem três grupos básicos de mecanismos de autenticação, que se utilizam de: aquilo que você é (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho), aquilo que apenas você possui (como seu cartão de senhas bancárias e um *token* gerador de senhas) e, finalmente, aquilo que apenas você sabe (como perguntas de segurança e suas senhas).

Uma senha, ou *password*, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a simplicidade que possui.

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha ela poderá usá-las para se passar por você na Internet e realizar ações em seu nome, como:

- acessar a sua conta de correio eletrônico e ler seus *e-mails*, enviar mensagens de *spam* e/ou contendo *phishing* e códigos maliciosos, furtar sua lista de contatos e pedir o reenvio de senhas de outras contas para este endereço de *e-mail* (e assim conseguir acesso a elas);
- acessar o seu computador e obter informações sensíveis nele armazenadas, como senhas e números de cartões de crédito;
- utilizar o seu computador para esconder a real identidade desta pessoa (o invasor) e, então, desferir ataques contra computadores de terceiros;
- acessar *sites* e alterar as configurações feitas por você, de forma a tornar públicas informações que deveriam ser privadas;
- acessar a sua rede social e usar a confiança que as pessoas da sua rede de relacionamento depositam em você para obter informações sensíveis ou para o envio de boatos, mensagens de *spam* e/ou códigos maliciosos.

8.1 Uso seguro de contas e senhas

Algumas das formas como a sua senha pode ser descoberta são:

- ao ser usada em computadores infectados. Muitos códigos maliciosos, ao infectar um computador, armazenam as teclas digitadas (inclusive senhas), espionam o teclado pela *webcam* (caso você possua uma e ela esteja apontada para o teclado) e gravam a posição da tela onde o *mouse* foi clicado (mais detalhes na Seção 4.4 do Capítulo Códigos maliciosos (*Malware*));
- ao ser usada em *sites* falsos. Ao digitar a sua senha em um *site* falso, achando que está no *site* verdadeiro, um atacante pode armazená-la e, posteriormente, usá-la para acessar o *site* verdadeiro e realizar operações em seu nome (mais detalhes na Seção 2.3 do Capítulo Golpes na Internet);
- por meio de tentativas de adivinhação (mais detalhes na Seção 3.5 do Capítulo Ataques na Internet);
- ao ser capturada enquanto trafega na rede, sem estar criptografada (mais detalhes na Seção 3.4 do Capítulo Ataques na Internet);
- por meio do acesso ao arquivo onde a senha foi armazenada caso ela não tenha sido gravada de forma criptografada (mais detalhes no Capítulo Criptografia);
- com o uso de técnicas de engenharia social, como forma a persuadi-lo a entregá-la voluntariamente;
- pela observação da movimentação dos seus dedos no teclado ou dos cliques do *mouse* em teclados virtuais.

Cuidados a serem tomados ao usar suas contas e senhas:

- certifique-se de não estar sendo observado ao digitar as suas senhas;
- não forneça as suas senhas para outra pessoa, em hipótese alguma;
- certifique-se de fechar a sua sessão ao acessar *sites* que requeiram o uso de senhas. Use a opção de sair (*logout*), pois isto evita que suas informações sejam mantidas no navegador;
- elabore boas senhas, conforme descrito na Seção 8.2;
- altere as suas senhas sempre que julgar necessário, conforme descrito na Seção 8.3;
- não use a mesma senha para todos os serviços que acessa (dicas de gerenciamento de senhas são fornecidas na Seção 8.4);
- ao usar perguntas de segurança para facilitar a recuperação de senhas, evite escolher questões cujas respostas possam ser facilmente adivinhadas (mais detalhes na Seção 8.5);
- certifique-se de utilizar serviços criptografados quando o acesso a um *site* envolver o fornecimento de senha (mais detalhes na Seção 10.1 do Capítulo Uso seguro da Internet);
- procure manter sua privacidade, reduzindo a quantidade de informações que possam ser coletadas sobre você, pois elas podem ser usadas para adivinhar a sua senha, caso você não tenha sido cuidadoso ao elaborá-la (mais detalhes no Capítulo Privacidade);
- mantenha a segurança do seu computador (mais detalhes no Capítulo Segurança de computadores);
- seja cuidadoso ao usar a sua senha em computadores potencialmente infectados ou comprometidos. Procure, sempre que possível, utilizar opções de navegação anônima (mais detalhes na Seção 12.3 do Capítulo Segurança de computadores).

8.2 Elaboração de senhas

Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

Alguns elementos que você **não deve** usar na elaboração de suas senhas são:

Qualquer tipo de dado pessoal: evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas[1] (estes dados podem ser facilmente obtidos e usados por pessoas que queiram tentar se autenticar como você).

Sequências de teclado: evite senhas associadas à proximidade entre os caracteres no teclado, como "`1qaz2wsx`" e "`QwerTAsdfG`", pois são bastante conhecidas e podem ser facilmente observadas ao serem digitadas.

[1] Qualquer data que possa estar relacionada a você, como a data de seu aniversário ou de seus familiares.

Palavras que façam parte de listas: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas (mais detalhes na Seção 3.5 do Capítulo Ataques na Internet).

Alguns elementos que você **deve** usar na elaboração de suas senhas são:

Números aleatórios: quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem **exclusivamente** caracteres numéricos.

Grande quantidade de caracteres: quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente.

Diferentes tipos de caracteres: quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Algumas dicas[2] práticas que você pode usar na elaboração de boas senhas são:

Selecione caracteres de uma frase: baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase "`O Cravo brigou com a Rosa debaixo de uma sacada`" você pode gerar a senha "`?OCbcaRddus`" (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).

Utilize uma frase longa: escolha uma frase longa, que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas à você (como o refrão de sua música preferida). Exemplo: se quando criança você sonhava em ser astronauta, pode usar como senha "`1 dia ainda verei os aneis de Saturno!!!`".

Faça substituições de caracteres: invente um padrão de substituição baseado, por exemplo, na semelhança visual ("`w`" e "`vv`") ou de fonética ("`ca`" e "`k`") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras "`s`" e "`r`", substituindo "`o`" por "`0`" (número zero) e usando a frase "`Sol, astro-rei do Sistema Solar`" você pode gerar a senha "`SS0l, asstrr0-rrei d0 SSisstema SS0larr`".

Existem serviços que permitem que você teste a complexidade de uma senha e que, de acordo com critérios, podem classificá-la como sendo, por exemplo, "`muito fraca`", "`fraca`", "`forte`" ou "`muito forte`". Ao usar estes serviços é importante ter em mente que, mesmo que uma senha tenha sido classificada como "`muito forte`", pode ser que ela não seja uma boa senha caso contenha dados pessoais que não são de conhecimento do serviço, mas que podem ser de conhecimento de um atacante.

Apenas você é capaz de definir se a senha elaborada é realmente boa!

[2] As senhas e os padrões usados para ilustrar as dicas, tanto nesta como nas versões anteriores da Cartilha, não devem ser usados pois já são de conhecimento público. Você deve adaptar estas dicas e criar suas próprias senhas e padrões.

8.3 Alteração de senhas

Você deve alterar a sua senha **imediatamente** sempre que desconfiar que ela pode ter sido descoberta ou que o computador no qual você a utilizou pode ter sido invadido ou infectado.

Algumas situações onde você deve alterar **rapidamente** a sua senha são:

- se um computador onde a senha esteja armazenada tenha sido furtado ou perdido;
- se usar um padrão para a formação de senhas e desconfiar que uma delas tenha sido descoberta. Neste caso, tanto o padrão como todas as senhas elaboradas com ele devem ser trocadas pois, com base na senha descoberta, um atacante pode conseguir inferir as demais;
- se utilizar uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles. Neste caso, esta senha deve ser alterada em todos os lugares nos quais é usada;
- ao adquirir equipamentos acessíveis via rede, como roteadores Wi-Fi, dispositivos *bluetooth* e *modems* ADSL (***A****symmetric* ***D****igital* ***S****ubscriber* ***L****ine*). Muitos destes equipamentos são configurados de fábrica com senha padrão, facilmente obtida em listas na Internet, e por isto, sempre que possível, deve ser alterada (mais detalhes no Capítulo Segurança de redes).

Nos demais casos é importante que a sua senha seja alterada **regularmente**, como forma de assegurar a confidencialidade. Não há como definir, entretanto, um período ideal para que a troca seja feita, pois depende diretamente de quão boa ela é e de quanto você a expõe (você a usa em computadores de terceiros? Você a usa para acessar outros *sites*? Você mantém seu computador atualizado?).

Não convém que você troque a senha em períodos muito curtos (menos de um mês, por exemplo) se, para conseguir se recordar, precisará elaborar uma senha fraca ou anotá-la em um papel e colá-lo no monitor do seu computador. Períodos muito longos (mais de um ano, por exemplo) também não são desejáveis pois, caso ela tenha sido descoberta, os danos causados podem ser muito grandes.

8.4 Gerenciamento de contas e senhas

Você já pensou em quantas contas e senhas diferentes precisa memorizar e combinar para acessar todos os serviços que utiliza e que exigem autenticação? Atualmente, confiar apenas na memorização pode ser algo bastante arriscado.

Para resolver este problema muitos usuários acabam usando técnicas que podem ser bastante perigosas e que, sempre que possível, devem ser evitadas. Algumas destas técnicas e os cuidados que você deve tomar caso, mesmo ciente dos riscos, opte por usá-las são:

Reutilizar as senhas: usar a mesma senha para acessar diferentes contas pode ser bastante arriscado, pois basta ao atacante conseguir a senha de uma conta para conseguir acessar as demais contas onde esta mesma senha foi usada.

- procure não usar a mesma senha para assuntos pessoais e profissionais;
- jamais reutilize senhas que envolvam o acesso a dados sensíveis, como as usadas em *Internet Banking* ou *e-mail*.

Usar opções como "Lembre-se de mim" e "Continuar conectado": o uso destas opções faz com que informações da sua conta de usuário sejam salvas em *cookies* que podem ser indevidamente coletados e permitam que outras pessoas se autentiquem como você.

- use estas opções somente nos *sites* nos quais o risco envolvido é bastante baixo;
- jamais as utilize em computadores de terceiros.

Salvar as senhas no navegador *Web*: esta prática é bastante arriscada, pois caso as senhas não estejam criptografadas com uma chave mestra, elas podem ser acessadas por códigos maliciosos, atacantes ou outras pessoas que venham a ter acesso ao computador.

- assegure-se de configurar uma chave mestra;
- seja bastante cuidadoso ao elaborar sua chave mestra, pois a segurança das demais senhas depende diretamente da segurança dela;
- **não esqueça sua chave mestra**.

Para não ter que recorrer a estas técnicas ou correr o risco de esquecer suas contas/senhas ou, pior ainda, ter que apelar para o uso de senhas fracas, você pode buscar o auxílio de algumas das formas de gerenciamento disponíveis.

Uma forma bastante simples de gerenciamento é listar suas contas/senhas em um papel e guardá-lo em um local seguro (como uma gaveta trancada). Neste caso, a segurança depende diretamente da dificuldade de acesso ao local escolhido para guardar este papel (de nada adianta colá-lo no monitor, deixá-lo embaixo do teclado ou sobre a mesa). Veja que é preferível usar este método a optar pelo uso de senhas fracas pois, geralmente, é mais fácil garantir que ninguém terá acesso físico ao local onde o papel está guardado do que evitar que uma senha fraca seja descoberta na Internet.

Caso você considere este método pouco prático, pode optar por outras formas de gerenciamento como as apresentadas a seguir, juntamente com alguns cuidados básicos que você deve ter ao usá-las:

Criar grupos de senhas, de acordo com o risco envolvido: você pode criar senhas únicas e bastante fortes e usá-las onde haja recursos valiosos envolvidos (por exemplo, para acesso a *Internet Banking* ou *e-mail*). Outras senhas únicas, porém um pouco mais simples, para casos nos quais o valor do recurso protegido é inferior (por exemplo, *sites* de comércio eletrônico, desde que suas informações de pagamento, como número de cartão de crédito, não sejam armazenadas para uso posterior) e outras simples e reutilizadas para acessos sem risco (como o cadastro para baixar um determinado arquivo).

- reutilize senhas apenas em casos nos quais o risco envolvido é bastante baixo.

Usar um programa gerenciador de contas/senhas: programas, como 1Password[3] e KeePass[4], permitem armazenar grandes quantidades de contas/senhas em um único arquivo, acessível por meio de uma chave mestra.

- seja bastante cuidadoso ao elaborar sua chave mestra, pois a segurança das demais senhas depende diretamente da segurança dela;

[3] 1Password - https://agilebits.com/onepassword.
[4] KeePass - http://keepass.info/.

- **não esqueça sua chave mestra** (sem ela, não há como você acessar os arquivos que foram criptografados, ou seja, todas as suas contas/senhas podem ser perdidas);
- assegure-se de obter o programa gerenciador de senhas de uma fonte confiável e de sempre mantê-lo atualizado;
- evite depender do programa gerenciador de senhas para acessar a conta do *e-mail* de recuperação (mais detalhes na Seção 8.5).

Gravar em um arquivo criptografado: você pode manter um arquivo criptografado em seu computador e utilizá-lo para cadastrar manualmente todas as suas contas e senhas.

- assegure-se de manter o arquivo sempre criptografado;
- assegure-se de manter o arquivo atualizado (sempre que alterar uma senha que esteja cadastrada no arquivo, você deve lembrar de atualizá-lo);
- faça *backup* do arquivo de senhas, para evitar perdê-lo caso haja problemas em seu computador.

8.5 Recuperação de senhas

Mesmo que você tenha tomado cuidados para elaborar a sua senha e utilizado mecanismos de gerenciamento, podem ocorrer casos, por inúmeros motivos, de você perdê-la. Para restabelecer o acesso perdido, alguns sistemas disponibilizam recursos como:

- permitir que você responda a uma pergunta de segurança previamente determinada por você;
- enviar a senha, atual ou uma nova, para o *e-mail* de recuperação previamente definido por você;
- confirmar suas informações cadastrais, como data de aniversário, país de origem, nome da mãe, números de documentos, etc;
- apresentar uma dica de segurança previamente cadastrada por você;
- enviar por mensagem de texto para um número de celular previamente cadastrado por você.

Todos estes recursos podem ser muito úteis, desde que cuidadosamente utilizados, pois assim como podem permitir que você recupere um acesso, também podem ser usados por atacantes que queiram se apossar da sua conta. Alguns cuidados que você deve tomar ao usá-los são:

- cadastre uma dica de segurança que seja vaga o suficiente para que ninguém mais consiga descobri-la e clara o bastante para que você consiga entendê-la. Exemplo: se sua senha for "`SS0l, asstrr0-rrei d0 SSisstema SS0larr`"[5], pode cadastrar a dica "`Uma das notas musicais`", o que o fará se lembrar da palavra "`Sol`" e se recordar da senha;

[5]Esta senha foi sugerida na Seção 8.2.

- seja cuidadoso com as informações que você disponibiliza em *blogs* e redes sociais, pois podem ser usadas por atacantes para tentar confirmar os seus dados cadastrais, descobrir dicas e responder perguntas de segurança (mais detalhes no Capítulo Privacidade);

- evite cadastrar perguntas de segurança que possam ser facilmente descobertas, como o nome do seu cachorro ou da sua mãe. Procure criar suas próprias perguntas e, de preferência, com respostas falsas. Exemplo: caso você tenha medo de altura, pode criar a pergunta "`Qual seu esporte favorito?`" e colocar como resposta "`paraquedismo`" ou "`alpinismo`";

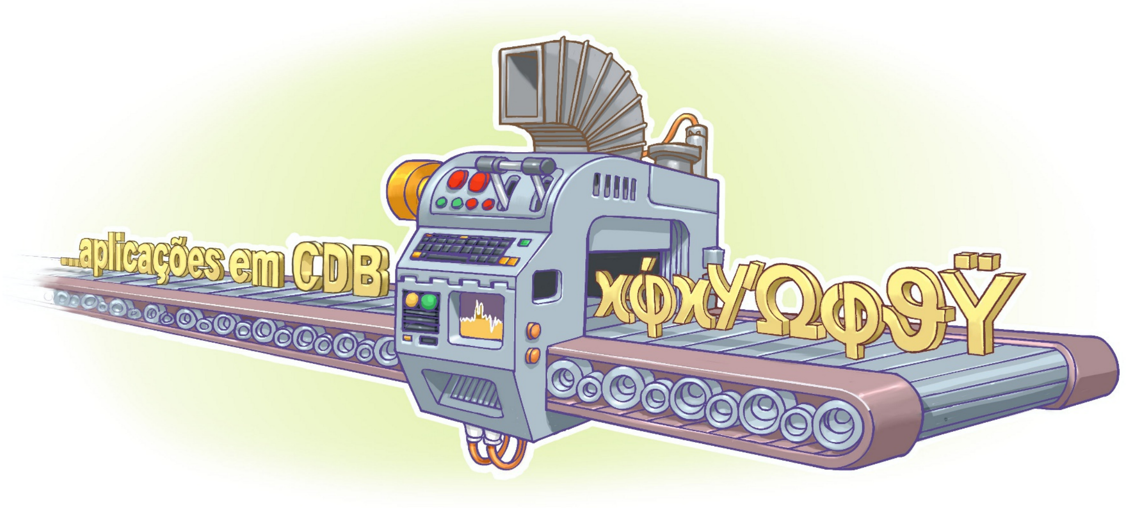
- ao receber senhas por *e-mail* procure alterá-las o mais rápido possível. Muitos sistemas enviam as senhas em texto claro, ou seja, sem nenhum tipo de criptografia e elas podem ser obtidas caso alguém tenha acesso à sua conta de *e-mail* ou utilize programas para interceptação de tráfego (mais detalhes na Seção 3.4 do Capítulo Ataques na Internet);

- procure cadastrar um *e-mail* de recuperação que você acesse regularmente, para não esquecer a senha desta conta também;

- procure não depender de programas gerenciadores de senhas para acessar o *e-mail* de recuperação (caso você esqueça sua chave mestra ou, por algum outro motivo, não tenha mais acesso às suas senhas, o acesso ao *e-mail* de recuperação pode ser a única forma de restabelecer os acessos perdidos);

- preste muita atenção ao cadastrar o *e-mail* de recuperação para não digitar um endereço que seja inválido ou pertencente a outra pessoa. Para evitar isto, muitos *sites* enviam uma mensagem de confirmação assim que o cadastro é realizado. Tenha certeza de recebê-la e de que as eventuais instruções de verificação tenham sido executadas.

9. Criptografia



A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

A primeira vista ela até pode parecer complicada, mas para usufruir dos benefícios que proporciona você não precisa estudá-la profundamente e nem ser nenhum matemático experiente. Atualmente, a criptografia já está integrada ou pode ser facilmente adicionada à grande maioria dos sistemas operacionais e aplicativos e para usá-la, muitas vezes, basta a realização de algumas configurações ou cliques de *mouse*.

Por meio do uso da criptografia você pode:

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger seus *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- proteger as comunicações realizadas pela Internet, como os *e-mails* enviados/recebidos e as transações bancárias e comerciais realizadas.

Nas próximas seções são apresentados alguns conceitos de criptografia. Antes, porém, é importante que você se familiarize com alguns termos geralmente usados e que são mostrados na Tabela 9.1.

Termo	Significado
Texto claro	Informação legível (original) que será protegida, ou seja, que será codificada
Texto codificado (cifrado)	Texto ilegível, gerado pela codificação de um texto claro
Codificar (cifrar)	Ato de transformar um texto claro em um texto codificado
Decodificar (decifrar)	Ato de transformar um texto codificado em um texto claro
Método criptográfico	Conjunto de programas responsável por codificar e decodificar informações
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de *bits*
Canal de comunicação	Meio utilizado para a troca de informações
Remetente	Pessoa ou serviço que envia a informação
Destinatário	Pessoa ou serviço que recebe a informação

Tabela 9.1: Termos empregados em criptografia e comunicações via Internet.

9.1 Criptografia de chave simétrica e de chaves assimétricas

De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Criptografia de chave simétrica: também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados.

Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Criptografia de chaves assimétricas: também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono.

Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido. Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:

- necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado) e;
- dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).

A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.

Para aproveitar as vantagens de cada um destes métodos, o ideal é o uso combinado de ambos, onde a criptografia de chave simétrica é usada para a codificação da informação e a criptografia de chaves assimétricas é utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão). Este uso combinado é o que é utilizado pelos navegadores *Web* e programas leitores de *e-mails*. Exemplos de uso deste método combinado são: SSL, PGP e S/MIME.

9.2 Função de resumo (*Hash*)

Uma função de resumo é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado *hash*[1].

Você pode utilizar *hash* para:

- verificar a integridade de um arquivo armazenado em seu computador ou em seus *backups*;
- verificar a integridade de um arquivo obtido da Internet (alguns *sites*, além do arquivo em si, também disponibilizam o *hash* correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado);
- gerar assinaturas digitais, como descrito na Seção 9.3.

Para verificar a integridade de um arquivo, por exemplo, você pode calcular o *hash* dele e, quando julgar necessário, gerar novamente este valor. Se os dois *hashes* forem iguais então você pode concluir que o arquivo não foi alterado. Caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado. Exemplos de métodos de *hash* são: SHA-1, SHA-256 e MD5.

9.3 Assinatura digital

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o *hash* e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda.

[1] O *hash* é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original e que qualquer alteração na informação original produzirá um *hash* distinto. Apesar de ser teoricamente possível que informações diferentes gerem *hashes* iguais, a probabilidade disto ocorrer é bastante baixa.

9.4 Certificado digital

Como dito anteriormente, a chave púbica pode ser livremente divulgada. Entretanto, se não houver como comprovar a quem ela pertence, pode ocorrer de você se comunicar, de forma cifrada, diretamente com um impostor.

Um impostor pode criar uma chave pública falsa para um amigo seu e enviá-la para você ou disponibilizá-la em um repositório. Ao usá-la para codificar uma informação para o seu amigo, você estará, na verdade, codificando-a para o impostor, que possui a chave privada correspondente e conseguirá decodificar. Uma das formas de impedir que isto ocorra é pelo uso de certificados digitais.

O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um *site Web*) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

Um certificado digital pode ser comparado a um documento de identidade, por exemplo, o seu passaporte, no qual constam os seus dados pessoais e a identificação de quem o emitiu. No caso do passaporte, a entidade responsável pela emissão e pela veracidade dos dados é a Polícia Federal. No caso do certificado digital esta entidade é uma Autoridade Certificadora (AC).

Uma AC emissora é também responsável por publicar informações sobre certificados que não são mais confiáveis. Sempre que a AC descobre ou é informada que um certificado não é mais confiável, ela o inclui em uma "lista negra", chamada de "Lista de Certificados Revogados" (LCR) para que os usuários possam tomar conhecimento. A LCR é um arquivo eletrônico publicado periodicamente pela AC, contendo o número de série dos certificados que não são mais válidos e a data de revogação.

A Figura 9.1 ilustra como os certificados digitais são apresentados nos navegadores *Web*. Note que, embora os campos apresentados sejam padronizados, a representação gráfica pode variar entre diferentes navegadores e sistemas operacionais. De forma geral, os dados básicos que compõem um certificado digital são:

- versão e número de série do certificado;
- dados que identificam a AC que emitiu o certificado;
- dados que identificam o dono do certificado (para quem ele foi emitido);
- chave pública do dono do certificado;
- validade do certificado (quando foi emitido e até quando é válido);
- assinatura digital da AC emissora e dados para verificação da assinatura.

O certificado digital de uma AC é emitido, geralmente, por outra AC, estabelecendo uma hierarquia conhecida como "cadeia de certificados" ou "caminho de certificação", conforme ilustrado na Figura 9.2. A AC raiz, primeira autoridade da cadeia, é a âncora de confiança para toda a hierarquia e, por não existir outra AC acima dela, possui um certificado autoassinado (mais detalhes a seguir). Os certificados das ACs raízes publicamente reconhecidas já vêm inclusos, por padrão, em grande parte dos sistemas operacionais e navegadores e são atualizados juntamente com os próprios sistemas. Alguns exemplos de atualizações realizadas na base de certificados dos navegadores são: inclusão de novas ACs, renovação de certificados vencidos e exclusão de ACs não mais confiáveis.

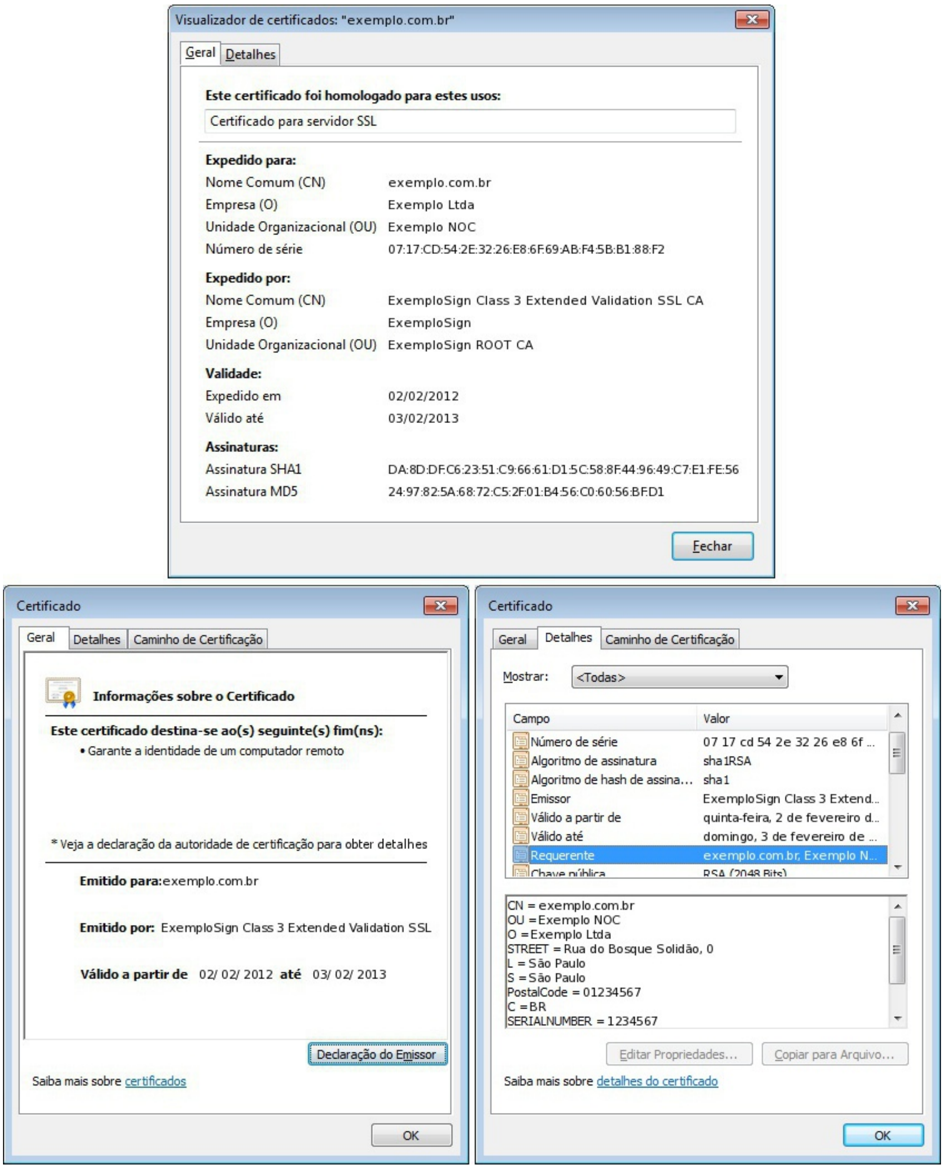


Figura 9.1: Exemplos de certificados digitais.

Alguns tipos especiais de certificado digital que você pode encontrar são:

Certificado autoassinado: é aquele no qual o dono e o emissor são a mesma entidade. Costuma ser usado de duas formas:

Legítima: além das ACs raízes, certificados autoassinados também costumam ser usados por instituições de ensino e pequenos grupos que querem prover confidencialidade e integridade nas conexões, mas que não desejam (ou não podem) arcar com o ônus de adquirir um certificado digital validado por uma AC comercial.

Maliciosa: um atacante pode criar um certificado autoassinado e utilizar, por exemplo, mensagens de *phishing* (mais detalhes na Seção 2.3 do Capítulo Golpes na Internet), para induzir os usuários a instalá-lo. A partir do momento em que o certificado for instalado no navegador, passa a ser possível estabelecer conexões cifradas com *sites* fraudulentos, sem que o navegador emita alertas quanto à confiabilidade do certificado.

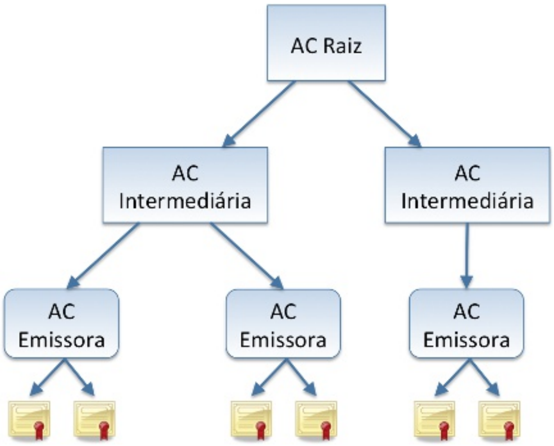


Figura 9.2: Cadeia de certificados.

Certificado EV SSL (*Extended Validation Secure Socket Layer*): certificado emitido sob um processo mais rigoroso de validação do solicitante. Inclui a verificação de que a empresa foi legalmente registrada, encontra-se ativa e que detém o registro do domínio para o qual o certificado será emitido, além de dados adicionais, como o endereço físico.

Dicas sobre como reconhecer certificados autoassinados e com validação avançada são apresentados na Seção 10.1 do Capítulo Uso seguro da Internet.

9.5 Programas de criptografia

Para garantir a segurança das suas mensagens é importante usar programas leitores de *e-mails* com suporte nativo a criptografia (por exemplo, que implementam S/MIME - ***S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtensions*) ou que permitam a integração de outros programas e complementos específicos para este fim.

Programas de criptografia, como o GnuPG[2], além de poderem ser integrados aos programas leitores de *e-mails*, também podem ser usados separadamente para cifrar outros tipos de informação, como os arquivos armazenados em seu computador ou em mídias removíveis.

Existem também programas (nativos do sistema operacional ou adquiridos separadamente) que permitem cifrar todo o disco do computador, diretórios de arquivos e dispositivos de armazenamento externo (como *pen-drives* e discos), os quais visam preservar o sigilo das informações em caso de perda ou furto do equipamento.

[2] `http://www.gnupg.org/`. O GnuPG não utiliza o conceito de certificados digitais emitidos por uma hierarquia de autoridades certificadoras. A confiança nas chaves é estabelecida por meio do modelo conhecido como "rede de confiança", no qual prevalece a confiança entre cada entidade.

9.6 Cuidados a serem tomados

Proteja seus dados:

- utilize criptografia sempre que, ao enviar uma mensagem, quiser assegurar-se que somente o destinatário possa lê-la;
- utilize assinaturas digitais sempre que, ao enviar uma mensagem, quiser assegurar ao destinatário que foi você quem a enviou e que o conteúdo não foi alterado;
- só envie dados sensíveis após certificar-se de que está usando uma conexão segura (mais detalhes na Seção 10.1 do Capítulo Uso seguro da Internet);
- utilize criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor;
- cifre o disco do seu computador e dispositivos removíveis, como disco externo e *pen-drive*. Desta forma, em caso de perda ou furto do equipamento, seus dados não poderão ser indevidamente acessados;
- verifique o *hash*, quando possível, dos arquivos obtidos pela Internet (isto permite que você detecte arquivos corrompidos ou que foram indevidamente alterados durante a transmissão).

Seja cuidadoso com as suas chaves e certificados:

- utilize chaves de tamanho adequado. Quanto maior a chave, mais resistente ela será a ataques de força bruta (mais detalhes na Seção 3.5 do Capítulo Ataques na Internet);
- não utilize chaves secretas óbvias (mais detalhes na Seção 8.2 do Capítulo Contas e senhas);
- certifique-se de não estar sendo observado ao digitar suas chaves e senhas de proteção;
- utilize canais de comunicação seguros quando compartilhar chaves secretas;
- armazene suas chaves privadas com algum mecanismo de proteção, como por exemplo senha, para evitar que outra pessoa faça uso indevido delas;
- preserve suas chaves. Procure fazer *backups* e mantenha-os em local seguro (se você perder uma chave secreta ou privada, não poderá decifrar as mensagens que dependiam de tais chaves);
- tenha muito cuidado ao armazenar e utilizar suas chaves em computadores potencialmente infectados ou comprometidos, como em *LAN houses*, *cybercafes*, *stands* de eventos, etc;
- se suspeitar que outra pessoa teve acesso à sua chave privada (por exemplo, porque perdeu o dispositivo em que ela estava armazenada ou porque alguém acessou indevidamente o computador onde ela estava guardada), solicite imediatamente a revogação do certificado junto à AC emissora.

Seja cuidadoso ao aceitar um certificado digital:

- mantenha seu sistema operacional e navegadores *Web* atualizados (além disto contribuir para a segurança geral do seu computador, também serve para manter as cadeias de certificados sempre atualizadas);
- mantenha seu computador com a data correta. Além de outros benefícios, isto impede que certificados válidos sejam considerados não confiáveis e, de forma contrária, que certificados não confiáveis sejam considerados válidos (mais detalhes no Capítulo Segurança de computadores);
- ao acessar um *site Web*, observe os símbolos indicativos de conexão segura e leia com atenção eventuais alertas exibidos pelo navegador (mais detalhes na Seção 10.1 do Capítulo Uso seguro da Internet);
- caso o navegador não reconheça o certificado como confiável, apenas prossiga com a navegação se tiver certeza da idoneidade da instituição e da integridade do certificado, pois, do contrário, poderá estar aceitando um certificado falso, criado especificamente para cometer fraudes (detalhes sobre como fazer isto na Seção 10.1.2 do Capítulo Uso seguro da Internet).

10. Uso seguro da Internet



A Internet traz inúmeras possibilidades de uso, porém para aproveitar cada uma delas de forma segura é importante que alguns cuidados sejam tomados. Além disto, como grande parte das ações realizadas na Internet ocorrem por intermédio de navegadores *Web* é igualmente importante que você saiba reconhecer os tipos de conexões existentes e verificar a confiabilidade dos certificados digitais antes de aceitá-los (detalhes sobre como fazer isto são apresentados na Seção 10.1).

Alguns dos principais usos e cuidados que você deve ter ao utilizar a Internet são:

Ao usar navegadores *Web*:

- mantenha-o atualizado, com a versão mais recente e com todas as atualizações aplicadas;
- configure-o para verificar automaticamente atualizações, tanto dele próprio como de complementos que estejam instalados;
- permita a execução de programas *Java* e *JavaScript*, porém assegure-se de utilizar complementos, como o NoScript (disponível para alguns navegadores), para liberar gradualmente a execução, conforme necessário, e apenas em *sites* confiáveis (mais detalhes na Seção 6.2 do Capítulo Outros riscos);

- permita que programas *ActiveX* sejam executados apenas quando vierem de *sites* conhecidos e confiáveis (mais detalhes também na Seção 6.2, do Capítulo Outros riscos);
- seja cuidadoso ao usar *cookies* caso deseje ter mais privacidade (mais detalhes na Seção 6.1 do Capítulo Outros riscos);
- caso opte por permitir que o navegador grave as suas senhas, tenha certeza de cadastrar uma chave mestra e de jamais esquecê-la (mais detalhes na Seção 8.4, do Capítulo Contas e senhas);
- mantenha seu computador seguro (mais detalhes no Capítulo Segurança de computadores).

Ao usar programas leitores de *e-mails*:

- mantenha-o atualizado, com a versão mais recente e com as todas atualizações aplicadas;
- configure-o para verificar automaticamente atualizações, tanto dele próprio como de complementos que estejam instalados;
- não utilize-o como navegador *Web* (desligue o modo de visualização no formato HTML);
- seja cuidadoso ao usar *cookies* caso deseje ter mais privacidade (mais detalhes na Seção 6.1 do Capítulo Outros riscos);
- seja cuidadoso ao clicar em *links* presentes em *e-mails* (se você realmente quiser acessar a página do *link*, digite o endereço diretamente no seu navegador *Web*);
- desconfie de arquivos anexados à mensagem mesmo que tenham sido enviados por pessoas ou instituições conhecidas (o endereço do remetente pode ter sido falsificado e o arquivo anexo pode estar infectado);
- antes de abrir um arquivo anexado à mensagem tenha certeza de que ele não apresenta riscos, verificando-o com ferramentas *antimalware*;
- verifique se seu sistema operacional está configurado para mostrar a extensão dos arquivos anexados;
- desligue as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
- desligue as opções de execução de *JavaScript* e de programas *Java*;
- habilite, se possível, opções para marcar mensagens suspeitas de serem fraude;
- use sempre criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor;
- mantenha seu computador seguro (mais detalhes no Capítulo Segurança de computadores).

Ao acessar *Webmails*:

- seja cuidadoso ao acessar a página de seu *Webmail* para não ser vítima de *phishing*. Digite a URL diretamente no navegador e tenha cuidado ao clicar em *links* recebidos por meio de mensagens eletrônicas (mais detalhes na Seção 2.3 do Capítulo Golpes na Internet);

- não utilize um *site* de busca para acessar seu *Webmail* (não há necessidade disto, já que URLs deste tipo são, geralmente, bastante conhecidas);
- seja cuidadoso ao elaborar sua senha de acesso ao *Webmail* para evitar que ela seja descoberta por meio de ataques de força bruta (mais detalhes na Seção 8.2 do Capítulo Contas e senhas);
- configure opções de recuperação de senha, como um endereço de *e-mail* alternativo, uma questão de segurança e um número de telefone celular (mais detalhes na Seção 8.5 do Capítulo Contas e senhas);
- evite acessar seu *Webmail* em computadores de terceiros e, caso seja realmente necessário, ative o modo de navegação anônima (mais detalhes na Seção 12.3 do Capítulo Segurança de computadores);
- certifique-se de utilizar conexões seguras sempre que acessar seu *Webmail*, especialmente ao usar redes Wi-Fi públicas. Se possível configure para que, por padrão, sempre seja utilizada conexão via "https" (mais detalhes na Seção 10.1);
- mantenha seu computador seguro (mais detalhes no Capítulo Segurança de computadores).

Ao efetuar transações bancárias e acessar *sites* de *Internet Banking*:

- certifique-se da procedência do *site* e da utilização de conexões seguras ao realizar transações bancárias via *Web* (mais detalhes na Seção 10.1);
- somente acesse *sites* de instituições bancárias digitando o endereço diretamente no navegador *Web*, nunca clicando em um *link* existente em uma página ou em uma mensagem;
- não utilize um *site* de busca para acessar o *site* do seu banco (não há necessidade disto, já que URLs deste tipo são, geralmente, bastante conhecidas);
- ao acessar seu banco, forneça apenas uma posição do seu cartão de segurança (desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição);
- não forneça senhas ou dados pessoais a terceiros, especialmente por telefone;
- desconsidere mensagens de instituições bancárias com as quais você não tenha relação, principalmente aquelas que solicitem dados pessoais ou a instalação de módulos de segurança;
- sempre que ficar em dúvida, entre em contato com a central de relacionamento do seu banco ou diretamente com o seu gerente;
- não realize transações bancárias por meio de computadores de terceiros ou redes Wi-Fi públicas;
- verifique periodicamente o extrato da sua conta bancária e do seu cartão de crédito e, caso detecte algum lançamento suspeito, entre em contato imediatamente com o seu banco ou com a operadora do seu cartão;
- antes de instalar um módulo de segurança, de qualquer *Internet Banking*, certifique-se de que o autor módulo é realmente a instituição em questão;
- mantenha seu computador seguro (mais detalhes no Capítulo Segurança de computadores).

Ao efetuar transações comerciais e acessar *sites* de comércio eletrônico:

- certifique-se da procedência do *site* e da utilização de conexões seguras ao realizar compras e pagamentos via *Web* (mais detalhes na Seção 10.1);
- somente acesse *sites* de comércio eletrônico digitando o endereço diretamente no navegador *Web*, nunca clicando em um *link* existente em uma página ou em uma mensagem;
- não utilize um *site* de busca para acessar o *site* de comércio eletrônico que você costuma acessar (não há necessidade disto, já que URLs deste tipo são, geralmente, bastante conhecidas);
- pesquise na Internet referências sobre o *site* antes de efetuar uma compra;
- desconfie de preços muito abaixo dos praticados no mercado;
- não realize compras ou pagamentos por meio de computadores de terceiros ou redes Wi-Fi públicas;
- sempre que ficar em dúvida, entre em contato com a central de relacionamento da empresa onde está fazendo a compra;
- verifique periodicamente o extrato da sua conta bancária e do seu cartão de crédito e, caso detecte algum lançamento suspeito, entre em contato imediatamente com o seu banco ou com a operadora do seu cartão de crédito;
- ao efetuar o pagamento de uma compra, nunca forneça dados de cartão de crédito em *sites* sem conexão segura ou em *e-mails* não criptografados;
- mantenha seu computador seguro (mais detalhes no Capítulo Segurança de computadores).

10.1 Segurança em conexões *Web*

Ao navegar na Internet, é muito provável que a grande maioria dos acessos que você realiza não envolva o tráfego de informações sigilosas, como quando você acessa *sites* de pesquisa ou de notícias. Esses acessos são geralmente realizados pelo protocolo HTTP, onde as informações trafegam em texto claro, ou seja, sem o uso de criptografia.

O protocolo HTTP, além de não oferecer criptografia, também não garante que os dados não possam ser interceptados, coletados, modificados ou retransmitidos e nem que você esteja se comunicando exatamente com o *site* desejado. Por estas características, ele não é indicado para transmissões que envolvem informações sigilosas, como senhas, números de cartão de crédito e dados bancários, e deve ser substituído pelo HTTPS, que oferece conexões seguras.

O protocolo HTTPS utiliza certificados digitais para assegurar a identidade, tanto do *site* de destino como a sua própria, caso você possua um. Também utiliza métodos criptográficos e outros protocolos, como o SSL (***S**ecure **S**ockets **L**ayer*) e o TLS (***T**ransport **L**ayer **S**ecurity*), para assegurar a confidencialidade e a integridade das informações.

Sempre que um acesso envolver a transmissão de informações sigilosas, é importante certificar-se do uso de conexões seguras. Para isso, você deve saber como identificar o tipo de conexão sendo

realizada pelo seu navegador *Web* e ficar atento aos alertas apresentados durante a navegação, para que possa, se necessário, tomar decisões apropriadas. Dicas para ajudá-lo nestas tarefas são apresentadas nas Seções 10.1.1 e 10.1.2.

10.1.1 Tipos de conexão

Para facilitar a identificação do tipo de conexão em uso você pode buscar auxílio dos mecanismos gráficos disponíveis nos navegadores *Web*[1] mais usados atualmente. Estes mecanismos, apesar de poderem variar de acordo com o fabricante de cada navegador, do sistema operacional e da versão em uso, servem como um forte indício do tipo de conexão sendo usada e podem orientá-lo a tomar decisões corretas.

De maneira geral, você vai se deparar com os seguintes tipos de conexões:

Conexão padrão: é a usada na maioria dos acessos realizados. Não provê requisitos de segurança. Alguns indicadores deste tipo de conexão, ilustrados na Figura 10.1, são:

- o endereço do *site* começa com "`http://`";
- em alguns navegadores, o tipo de protocolo usado (HTTP), por ser o padrão das conexões, pode ser omitido na barra de endereços;
- um símbolo do *site* (logotipo) é apresentado próximo à barra de endereço e, ao passar o *mouse* sobre ele, não é possível obter detalhes sobre a identidade do *site*.



Figura 10.1: Conexão não segura em diversos navegadores.

Conexão segura: é a que deve ser utilizada quando dados sensíveis são transmitidos, geralmente usada para acesso a *sites* de *Internet Banking* e de comércio eletrônico. Provê autenticação, integridade e confidencialidade, como requisitos de segurança. Alguns indicadores deste tipo de conexão, ilustrados na Figura 10.2, são:

- o endereço do *site* começa com "`https://`";
- o desenho de um "cadeado fechado" é mostrado na barra de endereço e, ao clicar sobre ele, detalhes sobre a conexão e sobre o certificado digital em uso são exibidos;
- um recorte colorido (branco ou azul) com o nome do domínio do *site* é mostrado ao lado da barra de endereço (à esquerda ou à direita) e, ao passar o *mouse* ou clicar sobre ele, são exibidos detalhes sobre conexão e certificado digital em uso[2].



Figura 10.2: Conexão segura em diversos navegadores.

Conexão segura com EV SSL: provê os mesmos requisitos de segurança que a conexão segura anterior, porém com maior grau de confiabilidade quanto à identidade do *site* e de seu dono, pois utiliza certificados EV SSL (mais detalhes na Seção 9.4 do Capítulo Criptografia). Além de apresentar indicadores similares aos apresentados na conexão segura sem o uso de EV SSL, também introduz um indicador próprio, ilustrado na Figura 10.3, que é:

- a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do *site*[3].



Figura 10.3: Conexão segura usando EV SSL em diversos navegadores.

Outro nível de proteção de conexão usada na Internet envolve o uso de certificados autoassinados e/ou cuja cadeia de certificação não foi reconhecida. Este tipo de conexão não pode ser caracterizado como sendo totalmente seguro (e nem totalmente inseguro) pois, apesar de prover integridade e confidencialidade, não provê autenticação, já que não há garantias relativas ao certificado em uso.

Quando você acessa um *site* utilizando o protocolo HTTPS, mas seu navegador não reconhece a cadeia de certificação, ele emite avisos como os descritos na Seção 10.1.2 e ilustrados na Figura 10.6. Caso você, apesar dos riscos, opte por aceitar o certificado, a simbologia mostrada pelo seu navegador será a ilustrada na Figura 10.4. Alguns indicadores deste tipo de conexão são:

- um cadeado com um "X" vermelho é apresentado na barra de endereço;

[1] A simbologia usada pelos navegadores *Web* pode ser diferente quando apresentada em dispositivos móveis.

[2] De maneira geral, as cores branco, azul e verde indicam que o *site* usa conexão segura. Ao passo que as cores amarelo e vermelho indicam que pode haver algum tipo de problema relacionado ao certificado em uso.

[3] As cores azul e branco indicam que o *site* possui um certificado de validação de domínio (a entidade dona do *site* detém o direito de uso do nome de domínio) e a cor verde indica que o *site* possui um certificado de validação estendida (a entidade dona do *site* detém o direito de uso do nome de domínio em questão e encontra-se legalmente registrada).

- a identificação do protocolo “https” é apresentado em vermelho e riscado;
- a barra de endereço muda de cor, ficando totalmente vermelha;
- um indicativo de erro do certificado é apresentado na barra de endereço;
- um recorte colorido com o nome do domínio do *site* ou da instituição (dona do certificado) é mostrado ao lado da barra de endereço e, ao passar o *mouse* sobre ele, é informado que uma exceção foi adicionada.

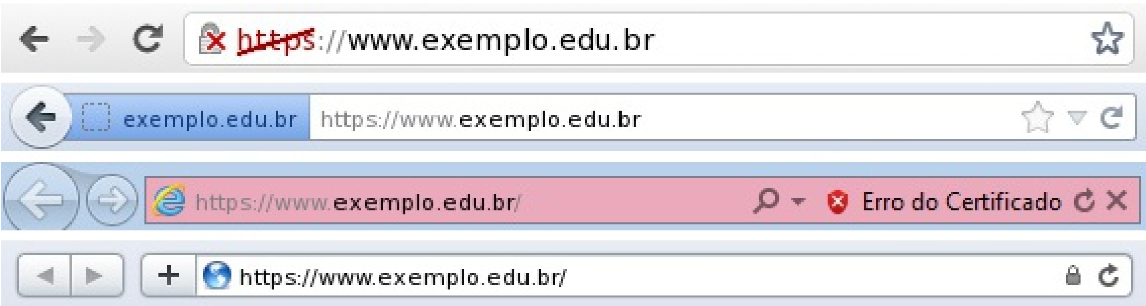


Figura 10.4: Conexão HTTPS com cadeia de certificação não reconhecida.

Certos *sites* fazem uso combinado, na mesma página *Web*, de conexão segura e não segura. Neste caso, pode ser que o cadeado desapareça, que seja exibido um ícone modificado (por exemplo, um cadeado com triângulo amarelo), que o recorte contendo informações sobre o *site* deixe de ser exibido ou ainda haja mudança de cor na barra de endereço, como ilustrado na Figura 10.5.



Figura 10.5: Uso combinado de conexão segura e não segura.

Mais detalhes sobre como reconhecer o tipo de conexão em uso podem ser obtidos em:

- Chrome - Como funcionam os indicadores de segurança do *website* (em português)
  `http://support.google.com/chrome/bin/answer.py?hl=pt-BR&answer=95617`
- Mozilla Firefox - *How do I tell if my connection to a website is secure?* (em inglês)
  `http://support.mozilla.org/en-US/kb/Site Identity Button`
- Internet Explorer - Dicas para fazer transações *online* seguras (em português)
  `http://windows.microsoft.com/pt-BR/windows7/Tips-for-making-secure-online-transaction-in-Internet-Explorer-9`
- Safari - *Using encryption and secure connections* (em inglês)
  `http://support.apple.com/kb/HT2573`

10.1.2 Como verificar se um certificado digital é confiável

Para saber se um certificado é confiável, é necessário observar alguns requisitos, dentre eles:

- se o certificado foi emitido por uma AC confiável (pertence a uma cadeia de confiança reconhecida);
- se o certificado está dentro do prazo de validade;
- se o certificado não foi revogado pela AC emissora;
- se o dono do certificado confere com a entidade com a qual está se comunicando (por exemplo: o nome do *site*).

Quando você tenta acessar um *site* utilizando conexão segura, normalmente seu navegador já realiza todas estas verificações. Caso alguma delas falhe, o navegador emite alertas semelhantes aos mostrados na Figura 10.6.

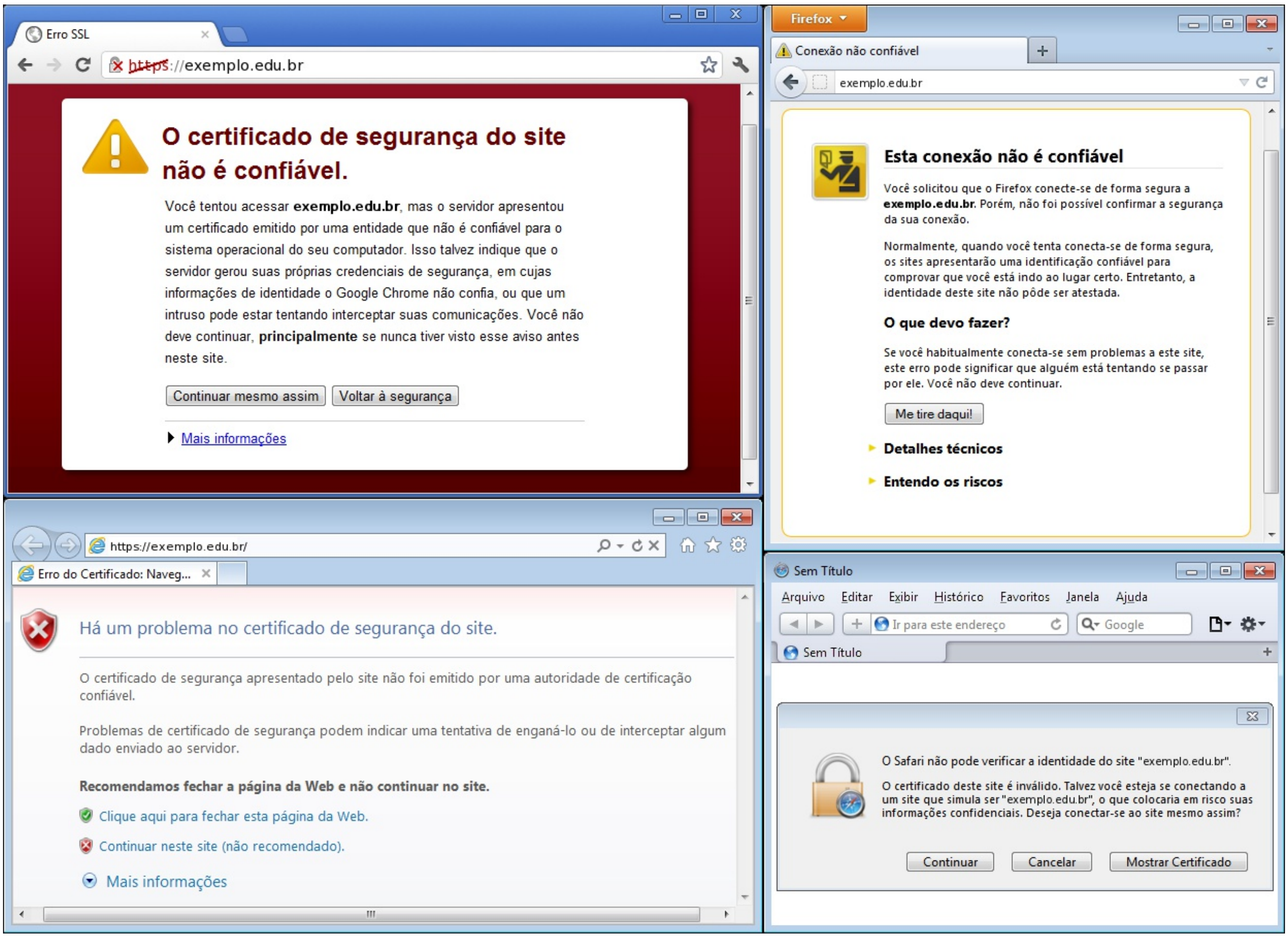


Figura 10.6: Alerta de certificado não confiável em diversos navegadores.

Em geral, alertas são emitidos em situações como:

- o certificado está fora do prazo de validade;
- o navegador não identificou a cadeia de certificação (dentre as possibilidades, o certificado pode pertencer a uma cadeia não reconhecida, ser autoassinado ou o navegador pode estar desatualizado e não conter certificados mais recentes de ACs);
- o endereço do *site* não confere com o descrito no certificado;
- o certificado foi revogado.

Ao receber os alertas do seu navegador você pode optar por:

Desistir da navegação: dependendo do navegador, ao selecionar esta opção você será redirecionado para uma página padrão ou a janela do navegador será fechada.

Solicitar detalhes sobre o problema: ao selecionar esta opção, detalhes técnicos serão mostrados e você pode usá-los para compreender o motivo do alerta e decidir qual opção selecionar.

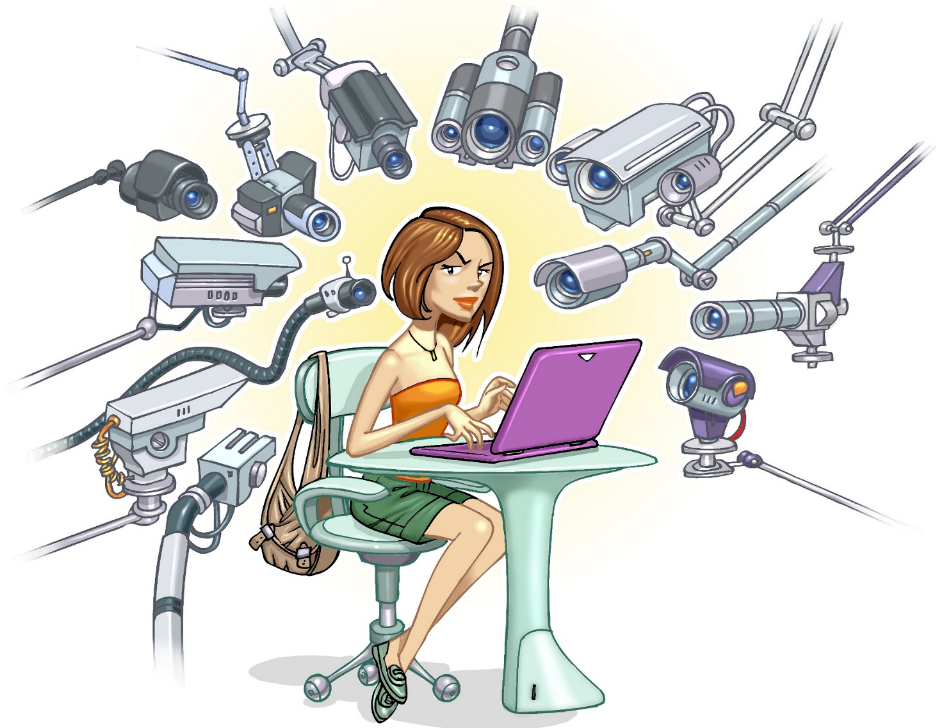
Aceitar os riscos: caso você, mesmo ciente dos riscos, selecione esta opção, a página desejada será apresentada e, dependendo do navegador, você ainda terá a opção de visualizar o certificado antes de efetivamente aceitá-lo e de adicionar uma exceção (permanente ou temporária).

Caso você opte por aceitar os riscos e adicionar uma exceção, é importante que, antes de enviar qualquer dado confidencial, verifique o conteúdo do certificado e observe:

- se o nome da instituição apresentado no certificado é realmente da instituição que você deseja acessar. Caso não seja, este é um forte indício de certificado falso;
- se as identificações de dono do certificado e da AC emissora são iguais. Caso sejam, este é um forte indício de que se trata de um certificado autoassinado. Observe que instituições financeiras e de comércio eletrônico sérias dificilmente usam certificados deste tipo;
- se o certificado encontra-se dentro do prazo de validade. Caso não esteja, provavelmente o certificado está expirado ou a data do seu computador não está corretamente configurada.

De qualquer modo, caso você receba um certificado desconhecido ao acessar um *site* e tenha alguma dúvida ou desconfiança, não envie qualquer informação para o *site* antes de entrar em contato com a instituição que o mantém para esclarecer o ocorrido.

11. Privacidade



Nada impede que você abdique de sua privacidade e, de livre e espontânea vontade, divulgue informações sobre você. Entretanto, há situações em que, mesmo que você queira manter a sua privacidade, ela pode ser exposta independente da sua vontade, por exemplo quando:

- outras pessoas divulgam informações sobre você ou imagens onde você está presente, sem a sua autorização prévia;
- alguém, indevidamente, coleta informações que trafegam na rede sem estarem criptografadas, como o conteúdo dos *e-mails* enviados e recebidos por você (mais detalhes na Seção 3.4 do Capítulo Ataques na Internet);
- um atacante ou um código malicioso obtém acesso aos dados que você digita ou que estão armazenados em seu computador (mais detalhes no Capítulo Códigos maliciosos (*Malware*));
- um atacante invade a sua conta de *e-mail* ou de sua rede social e acessa informações restritas;
- um atacante invade um computador no qual seus dados estão armazenados como, por exemplo, um servidor de *e-mails*[1];

[1]Normalmente existe um consenso ético entre administradores de redes e provedores de nunca lerem a caixa postal de um usuário sem o seu consentimento.

- seus hábitos e suas preferências de navegação são coletadas pelos *sites* que você acessa e repassadas para terceiros (mais detalhes na Seção 6.1 do Capítulo Outros riscos).

Para tentar proteger a sua privacidade na Internet há alguns cuidados que você deve tomar, como:

Ao acessar e armazenar seus *e-mails*:

- configure seu programa leitor de *e-mails* para não abrir imagens que não estejam na própria mensagem (o fato da imagem ser acessada pode ser usado para confirmar que o *e-mail* foi lido);
- utilize programas leitores de *e-mails* que permitam que as mensagens sejam criptografadas, de modo que apenas possam ser lidas por quem conseguir decodificá-las;
- armazene *e-mails* confidenciais em formato criptografado para evitar que sejam lidos por atacantes ou pela ação de códigos maliciosos (você pode decodificá-los sempre que desejar lê-los);
- utilize conexão segura sempre que estiver acessando seus *e-mails* por meio de navegadores *Web*, para evitar que eles sejam interceptados;
- utilize criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor;
- seja cuidadoso ao usar computadores de terceiros ou potencialmente infectados, para evitar que suas senhas sejam obtidas e seus *e-mails* indevidamente acessados;
- seja cuidadoso ao acessar seu *Webmail*, digite a URL diretamente no navegador e tenha cuidado ao clicar em *links* recebidos por meio de mensagens eletrônicas;
- mantenha seu computador seguro (mais detalhes no Capítulo Segurança de computadores).

Ao navegar na *Web*:

- seja cuidadoso ao usar *cookies*, pois eles podem ser usados para rastrear e manter as suas preferências de navegação, as quais podem ser compartilhadas entre diversos *sites* (mais detalhes na Seção 6.1 do Capítulo Outros riscos);
- utilize, quando disponível, navegação anônima, por meio de *anonymizers* ou de opções disponibilizadas pelos navegadores *Web* (chamadas de privativa ou "*InPrivate*"). Ao fazer isto, informações, como *cookies*, *sites* acessados e dados de formulários, não são gravadas pelo navegador *Web*;
- utilize, quando disponível, opções que indiquem aos *sites* que você não deseja ser rastreado ("*Do Not Track*"). Alguns navegadores oferecem configurações de privacidade que permitem que você informe aos *sites* que não deseja que informações que possam afetar sua privacidade sejam coletadas[2];
- utilize, quando disponível, listas de proteção contra rastreamento, que permitem que você libere ou bloqueie os *sites* que podem rastreá-lo;
- mantenha seu computador seguro (mais detalhes no Capítulo Segurança de computadores).

[2]Até o momento de escrita desta Cartilha, não existe um consenso sobre quais são essas informações. Além disto, as configurações de rastreamento servem como um indicativo ao *sites Web* e não há nada que os obrigue a respeitá-las.

Ao divulgar informações na *Web*:

- esteja atento e avalie com cuidado as informações divulgadas em sua página *Web* ou *blog*, pois elas podem não só ser usadas por alguém mal-intencionado, por exemplo, em um golpe de engenharia social, mas também para atentar contra a segurança do seu computador, ou mesmo contra a sua segurança física;
- procure divulgar a menor quantidade possível de informações, tanto sobre você como sobre seus amigos e familiares, e tente orientá-los a fazer o mesmo;
- sempre que alguém solicitar dados sobre você ou quando preencher algum cadastro, reflita se é realmente necessário que aquela empresa ou pessoa tenha acesso àquelas informações;
- ao receber ofertas de emprego pela Internet, que solicitem o seu currículo, tente limitar a quantidade de informações nele disponibilizada e apenas forneça mais dados quando estiver seguro de que a empresa e a oferta são legítimas;
- fique atento a ligações telefônicas e *e-mails* pelos quais alguém, geralmente falando em nome de alguma instituição, solicita informações pessoais sobre você, inclusive senhas;
- seja cuidadoso ao divulgar informações em redes sociais, principalmente aquelas envolvendo a sua localização geográfica pois, com base nela, é possível descobrir a sua rotina, deduzir informações (como hábitos e classe financeira) e tentar prever os próximos passos seus ou de seus familiares (mais detalhes na Seção 11.1).

11.1 Redes sociais



As redes sociais permitem que os usuários criem perfis e os utilizem para se conectar a outros usuários, compartilhar informações e se agrupar de acordo com interesses em comum. Alguns exemplos são: Facebook, Orkut, Twitter, Linkedin, Google+ e foursquare.

As redes sociais, atualmente, já fazem parte do cotidiano de grande parte do usuários da Internet, que as utilizam para se informar sobre os assuntos do momento e para saber o que seus amigos e ídolos estão fazendo, o que estão pensando e onde estão. Também são usadas para outros fins, como seleção de candidatos para vagas de emprego, pesquisas de opinião e mobilizações sociais.

As redes sociais possuem algumas características próprias que as diferenciam de outros meios de comunicação, como a velocidade com que as informações se propagam, a grande quantidade de pessoas que elas conseguem atingir e a riqueza de informações pessoais que elas disponibilizam. Essas características, somadas ao alto grau de confiança que os usuários costumam depositar entre si, fez com que as redes sociais chamassem a atenção, também, de pessoas mal-intencionadas.

Alguns dos principais riscos relacionados ao uso de redes sociais são:

Contato com pessoas mal-intencionadas: qualquer pessoa pode criar um perfil falso, tentando se passar por uma pessoa conhecida e, sem que saiba, você pode ter na sua rede (lista) de contatos pessoas com as quais jamais se relacionaria no dia a dia.

Furto de identidade: assim como você pode ter um impostor na sua lista de contatos, também pode acontecer de alguém tentar se passar por você e criar um perfil falso. Quanto mais informações você divulga, mais convincente o seu perfil falso poderá ser e maiores serão as chances de seus amigos acreditarem que estão realmente se relacionando com você.

Invasão de perfil: por meio de ataques de força bruta, do acesso a páginas falsas ou do uso de computadores infectados, você pode ter o seu perfil invadido. Atacantes costumam fazer isto para, além de furtar a sua identidade, explorar a confiança que a sua rede de contatos deposita em você e usá-la para o envio de *spam* e códigos maliciosos.

Uso indevido de informações: as informações que você divulga, além de poderem ser usadas para a criação de perfil falso, também podem ser usadas em ataques de força bruta, em golpes de engenharia social e para responder questões de segurança usadas para recuperação de senhas.

Invasão de privacidade: quanto maior a sua rede de contatos, maior é o número de pessoas que possui acesso ao que você divulga, e menores são as garantias de que suas informações não serão repassadas. Além disso, não há como controlar o que os outros divulgam sobre você.

Vazamento de informações: há diversos casos de empresas que tiveram o conteúdo de reuniões e detalhes técnicos de novos produtos divulgados na Internet e que, por isto, foram obrigadas a rever políticas e antecipar, adiar ou cancelar decisões.

Disponibilização de informações confidenciais: em uma troca "amigável" de mensagens você pode ser persuadido a fornecer seu *e-mail*, telefone, endereço, senhas, número do cartão de crédito, etc. As consequências podem ser desde o recebimento de mensagens indesejáveis até a utilização do número de seu cartão de crédito para fazer compras em seu nome.

Recebimento de mensagens maliciosas: alguém pode lhe enviar um arquivo contendo códigos maliciosos ou induzi-lo a clicar em um *link* que o levará a uma página *Web* comprometida.

Acesso a conteúdos impróprios ou ofensivos: como não há um controle imediato sobre o que as pessoas divulgam, pode ocorrer de você se deparar com mensagens ou imagens que contenham pornografia, violência ou que incitem o ódio e o racismo.

Danos à imagem e à reputação: calúnia e difamação podem rapidamente se propagar, jamais serem excluídas e causarem grandes danos às pessoas envolvidas, colocando em risco a vida profissional e trazendo problemas familiares, psicológicos e de convívio social. Também podem fazer com que empresas percam clientes e tenham prejuízos financeiros.

Sequestro: dados de localização podem ser usados por criminosos para descobrir a sua rotina e planejar o melhor horário e local para abordá-lo. Por exemplo: se você fizer *check-in* (se registrar no sistema) ao chegar em um cinema, um sequestrador pode deduzir que você ficará por lá cerca de 2 horas (duração média de um filme) e terá este tempo para se deslocar e programar o sequestro.

Furto de bens: quando você divulga que estará ausente por um determinado período de tempo para curtir as suas merecidas férias, esta informação pode ser usada por ladrões para saber quando e por quanto tempo a sua residência ficará vazia. Ao retornar, você pode ter a infeliz surpresa de descobrir que seus bens foram furtados.

A seguir, observe alguns cuidados que você deve ter ao usar as redes sociais.

Preserve a sua privacidade:

- considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa, tanto agora como futuramente;
- pense bem antes de divulgar algo, pois não há possibilidade de arrependimento. Uma frase ou imagem fora de contexto pode ser mal-interpretada e causar mal-entendidos. Após uma informação ou imagem se propagar, dificilmente ela poderá ser totalmente excluída;
- use as opções de privacidade oferecidas pelos *sites* e procure ser o mais restritivo possível (algumas opções costumam vir, por padrão, configuradas como públicas e devem ser alteradas);
- mantenha seu perfil e seus dados privados, permitindo o acesso somente a pessoas ou grupos específicos;
- procure restringir quem pode ter acesso ao seu endereço de *e-mail*, pois muitos *spammers* utilizam esses dados para alimentar listas de envio de *spam*;
- seja seletivo ao aceitar seus contatos, pois quanto maior for a sua rede, maior será o número de pessoas com acesso às suas informações. Aceite convites de pessoas que você realmente conheça e para quem contaria as informações que costuma divulgar;
- não acredite em tudo que você lê. Nunca repasse mensagens que possam gerar pânico ou afetar outras pessoas, sem antes verificar a veracidade da informação;
- seja cuidadoso ao se associar a comunidades e grupos, pois por meio deles muitas vezes é possível deduzir informações pessoais, como hábitos, rotina e classe social.

Seja cuidadoso ao fornecer a sua localização:

- observe o fundo de imagens (como fotos e vídeos), pois podem indicar a sua localização;
- não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência;
- ao usar redes sociais baseadas em geolocalização, procure se registrar (fazer *check-in*) em locais movimentados e nunca em locais considerados perigosos;
- ao usar redes sociais baseadas em geolocalização, procure fazer *check-in* quando sair do local, ao invés de quando chegar.

Respeite a privacidade alheia:

- não divulgue, sem autorização, imagens em que outras pessoas apareçam;
- não divulgue mensagens ou imagens copiadas do perfil de pessoas que restrinjam o acesso;
- seja cuidadoso ao falar sobre as ações, hábitos e rotina de outras pessoas;
- tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público.

Previna-se contra códigos maliciosos e *phishing*:

- mantenha o seu computador seguro, com os programas atualizados e com todas as atualizações aplicadas (mais detalhes no Capítulo Segurança de computadores);
- utilize e mantenha atualizados mecanismos de proteção, como *antimalware* e *firewall* pessoal (mais detalhes no Capítulo Mecanismos de segurança);
- desconfie de mensagens recebidas mesmo que tenham vindo de pessoas conhecidas, pois elas podem ter sido enviadas de perfis falsos ou invadidos;
- seja cuidadoso ao acessar *links* reduzidos. Há *sites* e complementos para o seu navegador que permitem que você expanda o *link* antes de clicar sobre ele (mais detalhes na Seção 7.10 do Capítulo Mecanismos de segurança).

Proteja o seu perfil:

- seja cuidadoso ao usar e ao elaborar as suas senhas (mais detalhes no Capítulo Contas e senhas);
- habilite, quando disponível, as notificações de *login*, pois assim fica mais fácil perceber se outras pessoas estiverem utilizando indevidamente o seu perfil;
- use sempre a opção de *logout* para não esquecer a sessão aberta;
- denuncie casos de abusos, como imagens indevidas e perfis falsos ou invadidos.

Proteja sua vida profissional:

- cuide da sua imagem profissional. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode atrapalhar um processo seletivo que você venha a participar (muitas empresas consultam as redes sociais à procura de informações sobre os candidatos, antes de contratá-los);
- verifique se sua empresa possui um código de conduta e procure estar ciente dele. Observe principalmente as regras relacionadas ao uso de recursos e divulgação de informações;
- evite divulgar detalhes sobre o seu trabalho, pois isto pode beneficiar empresas concorrentes e colocar em risco o seu emprego;
- preserve a imagem da sua empresa. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode prejudicar a imagem e os negócios da empresa e, indiretamente, você mesmo;
- proteja seu emprego. Sua rede de contatos pode conter pessoas do círculo profissional que podem não gostar de saber que, por exemplo, a causa do seu cansaço ou da sua ausência é aquela festa que você foi e sobre a qual publicou diversas fotos;
- use redes sociais ou círculos distintos para fins específicos. Você pode usar, por exemplo, uma rede social para amigos e outra para assuntos profissionais ou separar seus contatos em diferentes grupos, de forma a tentar restringir as informações de acordo com os diferentes tipos de pessoas com os quais você se relaciona;

Proteja seus filhos:

- procure deixar seus filhos conscientes dos riscos envolvidos no uso das redes sociais;
- procure respeitar os limites de idade estipulados pelos *sites* (eles não foram definidos à toa);
- oriente seus filhos para não se relacionarem com estranhos e para nunca fornecerem informações pessoais, sobre eles próprios ou sobre outros membros da família;
- oriente seus filhos a não divulgarem informações sobre hábitos familiares e nem de localização (atual ou futura);
- oriente seus filhos para jamais marcarem encontros com pessoas estranhas;
- oriente seus filhos sobre os riscos de uso da *webcam* e que eles nunca devem utilizá-la para se comunicar com estranhos;
- procure deixar o computador usado pelos seus filhos em um local público da casa (dessa forma, mesmo a distância, é possível observar o que eles estão fazendo e verificar o comportamento deles).

12. Segurança de computadores



Muito provavelmente é em seu computador pessoal que a maioria dos seus dados está gravada e, por meio dele, que você acessa *e-mails* e redes sociais e realiza transações bancárias e comerciais. Por isto, mantê-lo seguro é essencial para se proteger dos riscos envolvidos no uso da Internet.

Além disto, ao manter seu computador seguro, você diminui as chances dele ser indevidamente utilizado para atividades maliciosas, como disseminação de *spam*, propagação de códigos maliciosos e participação em ataques realizados via Internet.

Muitas vezes, os atacantes estão interessados em conseguir o acesso à grande quantidade de computadores, independente de quais são e das configurações que possuem. Por isto, acreditar que seu computador está protegido por não apresentar atrativos para um atacante pode ser um grande erro.

Para manter seu computador pessoal seguro, é importante que você:

Mantenha os programas instalados com as versões mais recentes:

Fabricantes costumam lançar novas versões quando há recursos a serem adicionados e vulnerabilidades a serem corrigidas. Sempre que uma nova versão for lançada, ela deve ser prontamente instalada, pois isto pode ajudar a proteger seu computador da ação de atacantes e códigos maliciosos.

Além disto, alguns fabricantes deixam de dar suporte e de desenvolver atualizações para versões antigas, o que significa que vulnerabilidades que possam vir a ser descobertas não serão corrigidas.

- remova programas que você não utiliza mais. Programas não usados tendem a ser esquecidos e a ficar com versões antigas (e potencialmente vulneráveis);
- remova as versões antigas. Existem programas que permitem que duas ou mais versões estejam instaladas ao mesmo tempo. Nestes casos, você deve manter apenas a versão mais recente e remover as mais antigas;
- tenha o hábito de verificar a existência de novas versões, por meio de opções disponibilizadas pelos próprios programas ou acessando diretamente os *sites* dos fabricantes.

Mantenha os programas instalados com todas as atualizações aplicadas:

Quando vulnerabilidades são descobertas, certos fabricantes costumam lançar atualizações específicas, chamadas de *patches*, *hot fixes* ou *service packs*. Portanto, para manter os programas instalados livres de vulnerabilidades, além de manter as versões mais recentes, é importante que sejam aplicadas todas as atualizações disponíveis.



- configure, quando possível, para que os programas sejam atualizados automaticamente;
- programe as atualizações automáticas para serem baixadas e aplicadas em horários em que seu computador esteja ligado e conectado à Internet. Alguns programas, por padrão, são configurados para que as atualizações sejam feitas de madrugada, período no qual grande parte dos computadores está desligada (as atualizações que não foram feitas no horário programado podem não ser feitas quando ele for novamente ligado);
- no caso de programas que não possuam o recurso de atualização automática, ou caso você opte por não utilizar este recurso, é importante visitar constantemente os *sites* dos fabricantes para verificar a existência de novas atualizações;
- utilize programas para verificação de vulnerabilidades, como o PSI (mais detalhes na Seção 7.10 do Capítulo Mecanismos de segurança), para verificar se os programas instalados em seu computador estão atualizados.

Use apenas programas originais:

O uso de programas não originais pode colocar em risco a segurança do seu computador já que muitos fabricantes não permitem a realização de atualizações quando detectam versões não licenciadas. Além disto, a instalação de programas deste tipo, obtidos de mídias e *sites* não confiáveis ou via programas de compartilhamento de arquivos, pode incluir a instalação de códigos maliciosos.

- ao adquirir computadores com programas pré-instalados, procure certificar-se de que eles são originais solicitando ao revendedor as licenças de uso;
- ao enviar seu computador para manutenção, não permita a instalação de programas que não sejam originais;

- caso deseje usar um programa proprietário, mas não tenha recursos para adquirir a licença, procure por alternativas gratuitas ou mais baratas e que apresentem funcionalidades semelhantes as desejadas.



Use mecanismos de proteção:

O uso de mecanismos de proteção, como programas *antimalware* e *firewall* pessoal, pode contribuir para que seu computador não seja infectado/invadido e para que não participe de atividades maliciosas.

- utilize mecanismos de segurança, como os descritos no Capítulo Mecanismos de segurança;
- mantenha seu *antimalware* atualizado, incluindo o arquivo de assinaturas;
- assegure-se de ter um *firewall* pessoal instalado e ativo em seu computador;
- crie um disco de emergência e o utilize quando desconfiar que o *antimalware* instalado está desabilitado/comprometido ou que o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência, etc.);
- verifique periodicamente os *logs* gerados pelo seu *firewall* pessoal, sistema operacional e *antimalware* (observe se há registros que possam indicar algum problema de segurança).

Use as configurações de segurança já disponíveis:

Muitos programas disponibilizam opções de segurança, mas que, por padrão, vêm desabilitadas ou em níveis considerados baixos. A correta configuração destas opções pode contribuir para melhorar a segurança geral do seu computador.

- observe as configurações de segurança e privacidade oferecidas pelos programas instalados em seu computador (como programas leitores de *e-mails* e navegadores *Web*) e altere-as caso não estejam de acordo com as suas necessidades.

Seja cuidadoso ao manipular arquivos:

Alguns mecanismos, como os programas *antimalware*, são importantes para proteger seu computador contra ameaças já conhecidas, mas podem não servir para aquelas ainda não detectadas. Novos códigos maliciosos podem surgir, a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança e, por isto, adotar uma postura preventiva é tão importante quanto as outras medidas de segurança aplicadas.

- seja cuidadoso ao clicar em *links*, independente de como foram recebidos e de quem os enviou;
- seja cuidadoso ao clicar em *links* curtos, procure usar complementos que possibilitem que o *link* de destino seja visualizado;
- não considere que mensagens vindas de conhecidos são sempre confiáveis, pois o campo de remetente pode ter sido falsificado ou elas podem ter sido enviadas de contas falsas ou invadidas;
- desabilite, em seu seu programa leitor de *e-mails*, a auto-execução de arquivos anexados;

- desabilite a auto-execução de mídias removíveis (se estiverem infectadas, elas podem comprometer o seu computador ao serem executadas);
- não abra ou execute arquivos sem antes verificá-los com seu *antimalware*;
- configure seu *antimalware* para verificar todos os formatos de arquivo pois, apesar de inicialmente algumas extensões terem sido mais usadas para a disseminação de códigos maliciosos, atualmente isso já não é mais válido;
- tenha cuidado com extensões ocultas. Alguns sistemas possuem como configuração padrão ocultar a extensão de tipos de arquivos conhecidos. Exemplo: se um atacante renomear o arquivo "`exemplo.scr`" para "`exemplo.txt.scr`", ao ser visualizado o nome do arquivo será mostrado como "`exemplo.txt`", já que a extensão "`.scr`" não será mostrada.

Alguns cuidados especiais para manipular arquivos contendo macros são:

- verifique o nível de segurança associado à execução de macros e certifique-se de associar um nível que, no mínimo, pergunte antes de executá-las (normalmente associado ao nível médio);
- permita a execução de macros apenas quando realmente necessário (caso não tenha certeza, é melhor não permitir a execução);
- utilize visualizadores. Arquivos gerados, por exemplo, pelo Word, PowerPoint e Excel podem ser visualizados e impressos, sem que as macros sejam executadas, usando visualizadores gratuitos disponibilizados no *site* do fabricante.

Proteja seus dados:

O seu computador pessoal é, provavelmente, onde a maioria dos seus dados fica gravada. Por este motivo, é importante que você tome medidas preventivas para evitar perdê-los.

- faça regularmente *backup* dos seus dados. Para evitar que eles sejam perdidos em caso de furto ou mal-funcionamento do computador (por exemplo, invasão, infecção por códigos maliciosos ou problemas de *hardware*;
- siga as dicas relacionadas a *backups* apresentadas na Seção 7.5 do Capítulo Mecanismos de segurança.

Mantenha seu computador com a data e a hora corretas:

A data e a hora do seu computador são usadas na geração de *logs*, na correlação de incidentes de segurança, na verificação de certificados digitais (para conferir se estão válidos). Portanto, é muito importante que tome medidas para garantir que estejam sempre corretas.

- observe as dicas sobre como manter a hora do seu computador sincronizado apresentadas em `http://ntp.br/`.

Crie um disco de recuperação de sistema:

Discos de recuperação são úteis em caso de emergência, como atualizações mal-sucedidas ou desligamentos abruptos que tenham corrompido arquivos essenciais ao funcionamento do sistema (causado geralmente por queda de energia). Além disso, também podem socorrer caso seu computador seja infectado e o código malicioso tenha apagado arquivos essenciais. Podem ser criados por meio de opções do sistema operacional ou de programas *antimalware* que ofereçam esta funcionalidade.

- crie um disco de recuperação do seu sistema e certifique-se de tê-lo sempre por perto, no caso de emergências.

Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros:

- ao instalar *plug-ins*, complementos e extensões, procure ser bastante criterioso e siga as dicas de prevenção apresentadas na Seção 6.4 do Capítulo Outros riscos.

Seja cuidadoso ao enviar seu computador para serviços de manutenção:

- procure selecionar uma empresa com boas referências;
- pesquise na Internet sobre a empresa, à procura de opinião de clientes sobre ela;
- não permita a instalação de programas não originais;
- se possível, faça *backups* dos seus dados antes de enviar seu computador, para não correr o risco de perdê-los acidentalmente ou como parte do processo de manutenção do seu computador;
- se possível, peça que a manutenção seja feita em sua residência, assim fica mais fácil de acompanhar a realização do serviço.

Seja cuidadoso ao utilizar o computador em locais públicos:

Quando usar seu computador em público, é importante tomar cuidados para evitar que ele seja furtado ou indevidamente utilizado por outras pessoas.

- procure manter a segurança física do seu computador, utilizando travas que dificultem que ele seja aberto, que tenha peças retiradas ou que seja furtado, como cadeados e cabos de aço;
- procure manter seu computador bloqueado, para evitar que seja usado quando você não estiver por perto (isso pode ser feito utilizando protetores de tela com senha ou com programas que impedem o uso do computador caso um dispositivo específico não esteja conectado);
- configure seu computador para solicitar senha na tela inicial (isso impede que alguém reinicie seu computador e o acesse diretamente);
- utilize criptografia de disco para que, em caso de perda ou furto, seus dados não sejam indevidamente acessados.

12.1 Administração de contas de usuários

A maioria dos sistemas operacionais possui 3 tipos de conta de usuário:

Administrador (*administrator*, *admin* ou *root*): fornece controle completo sobre o computador, devendo ser usada para atividades como criar/alterar/excluir outras contas, instalar programas de uso geral e alterar de configuração que afetem os demais usuários ou o sistema operacional.

Padrão (*standard*, limitada ou *limited*): considerada de uso "normal" e que contém os privilégios que a grande maioria dos usuários necessita para realizar tarefas rotineiras, como alterar configurações pessoais, navegar, ler *e-mails*, redigir documentos, etc.

Convidado (*guest*): destinada aos usuários eventuais, não possui senha e não pode ser acessada remotamente. Permite que o usuário realize tarefas como navegar na Internet e executar programas já instalados. Quando o usuário que utilizou esta conta deixa de usar o sistema, todas as informações e arquivos que foram criados referentes a ela são apagados.

Quando um programa é executado, ele herda as permissões da conta do usuário que o executou e pode realizar operações e acessar arquivos de acordo com estas permissões. Se o usuário em questão estiver utilizando a conta de administrador, então o programa poderá executar qualquer tipo de operação e acessar todo tipo de arquivo.

A conta de administrador, portanto, deve ser usada apenas em situações nas quais uma conta padrão não tenha privilégios suficientes para realizar uma operação[1]. E, sobretudo, pelo menor tempo possível. Muitas pessoas, entretanto, por questões de comodidade ou falta de conhecimento, utilizam esta conta para realizar todo tipo de atividade.

Utilizar nas atividades cotidianas uma conta com privilégios de administrador é um hábito que deve ser evitado, pois você pode, por exemplo, apagar acidentalmente arquivos essenciais para o funcionamento do sistema operacional ou instalar inadvertidamente um código malicioso, que terá acesso irrestrito ao seu computador.

Alguns cuidados específicos referentes à administração de contas em computadores pessoais são:

- nunca compartilhe a senha de administrador;
- crie uma conta padrão e a utilize para a realização de suas tarefas rotineiras;
- utilize a conta de administrador apenas o mínimo necessário;
- use a opção de "executar como administrador" quando necessitar de privilégios administrativos;
- crie tantas contas padrão quantas forem as pessoas que utilizem o seu computador;
- assegure que todas as contas existentes em seu computador tenham senha;
- mantenha a conta de convidado sempre desabilitada (caso você queira utilizá-la, libere-a pelo tempo necessário, mas tenha certeza de novamente bloqueá-la quando não estiver mais em uso);

[1]Esta recomendação baseia-se em um princípio de segurança conhecido como "privilégio mínimo" e visa evitar danos por uso equivocado ou não autorizado.

- assegure que o seu computador esteja configurado para solicitar a conta de usuário e a senha na tela inicial;
- assegure que a opção de *login* (inicio de sessão) automático esteja desabilitada;
- não crie e não permita o uso de contas compartilhadas, cada conta deve ser acessada apenas por uma pessoa (assim é possível rastrear as ações realizadas por cada um e detectar uso indevido);
- crie tantas contas com privilégio de administrador quantas forem as pessoas que usem o seu computador e que necessitem destes privilégios.

12.2 O que fazer se seu computador for comprometido

Há alguns indícios que, isoladamente ou em conjunto, podem indicar que seu computador foi comprometido. Alguns deles são:

- o computador desliga sozinho e sem motivo aparente;
- o computador fica mais lento, tanto para ligar e desligar como para executar programas;
- o acesso à Internet fica mais lento;
- o acesso ao disco se torna muito frequente;
- janelas de *pop-up* aparecem de forma inesperada;
- mensagens de *logs* são geradas em excesso ou deixam de ser geradas;
- arquivos de *logs* são apagados, sem nenhum motivo aparente;
- atualizações do sistema operacional ou do *antimalware* não podem ser aplicadas.

Caso perceba estes indícios em seu computador e conclua que ele possa estar infectado ou invadido, é importante que você tome medidas para tentar reverter os problemas. Para isto, os seguintes passos devem ser executados por você:

a. Certifique-se de que seu computador esteja atualizado (com a versão mais recente e com todas as atualizações aplicadas). Caso não esteja, atualize-o imediatamente;

b. certifique-se de que seu *antimalware* esteja sendo executado e atualizado, incluindo o arquivo de assinaturas;

c. execute o *antimalware*, configurando-o para verificar todos os discos e analisar todas as extensões de arquivos;

d. limpe os arquivos que o *antimalware* detectar como infectado caso haja algum;

e. caso deseje, utilize outro *antimalware* como, por exemplo, uma versão *online* (neste caso, certifique-se de temporariamente interromper a execução do *antimalware* local).

Executar estes passos, na maioria das vezes, consegue resolver grande parte dos problemas relacionados a códigos maliciosos. É necessário, porém, que você verifique se seu computador não foi invadido e, para isto, você deve seguir os seguintes passos:

a. Certifique-se de que seu *firewall* pessoal esteja ativo;

b. verifique os *logs* do seu *firewall* pessoal. Caso encontre algo fora do padrão e que o faça concluir que seu computador tenha sido invadido, o melhor a ser feito é reinstalá-lo, pois dificilmente é possível determinar com certeza as ações do invasor;

c. antes de reinstalá-lo, faça *backups* de *logs* e notifique ao CERT.br sobre a ocorrência (mais detalhes na Seção 7.2 do Capítulo Mecanismos de segurança);

d. reinstale o sistema operacional e aplique todas as atualizações, principalmente as de segurança;

e. instale e atualize o seu programa *antimalware*;

f. instale ou ative o seu *firewall* pessoal;

g. recupere seus dados pessoais, por meio de um *backup* confiável.

Independente de seu computador ter sido infectado ou invadido, é importante alterar rapidamente todas as senhas dos serviços que você costuma acessar por meio dele.

12.3 Cuidados ao usar computadores de terceiros

Ao usar outros computadores, seja de seus amigos, na sua escola, em *lanhouse* e *cyber* café, é necessário que os cuidados com segurança sejam redobrados. Ao passo que no seu computador é possível tomar medidas preventivas para evitar os riscos de uso da Internet, ao usar um outro computador não há como saber, com certeza, se estes mesmos cuidados estão sendo devidamente tomados e quais as atitudes dos demais usuários. Alguns cuidados que você deve ter são:

- utilize opções de navegar anonimamente, caso queria garantir sua privacidade (você pode usar opções do próprio navegador *Web* ou *anonymizers*);
- utilize um *antimalware online* para verificar se o computador está infectado;
- não efetue transações bancárias ou comerciais;
- não utilize opções como "Lembre-se de mim" e "Continuar conectado";
- não permita que suas senhas sejam memorizadas pelo navegador *Web*;
- limpe os dados pessoais salvos pelo navegador, como histórico de navegação e *cookies* (os navegadores disponibilizam opções que permitem que isto seja facilmente realizado);
- assegure-se de sair (*logout*) de sua conta de usuário, nos *sites* que você tenha acessado;
- seja cuidadoso ao conectar mídias removíveis, como *pen-drives*. Caso você use seu *pen-drive* no computador de outra pessoa, assegure-se de verificá-lo com seu *antimalware* quando for utilizá-lo em seu computador;
- ao retornar ao seu computador, procure alterar as senhas que, por ventura, você tenha utilizado.

13. Segurança de redes



Inicialmente, grande parte dos acessos à Internet eram realizados por meio de conexão discada com velocidades que dificilmente ultrapassavam 56 Kbps. O usuário, de posse de um *modem* e de uma linha telefônica, se conectava ao provedor de acesso e mantinha esta conexão apenas pelo tempo necessário para realizar as ações que dependessem da rede.

Desde então, grandes avanços ocorreram e novas alternativas surgiram, sendo que atualmente grande parte dos computadores pessoais ficam conectados à rede pelo tempo em que estiverem ligados e a velocidades que podem chegar a até 100 Mbps[1]. Conexão à Internet também deixou de ser um recurso oferecido apenas a computadores, visto a grande quantidade de equipamentos com acesso à rede, como dispositivos móveis, TVs, eletrodomésticos e sistemas de áudio.

Independente do tipo de tecnologia usada, ao conectar o seu computador à rede ele pode estar sujeito a ameaças, como:

Furto de dados: informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador.

[1]Estes dados baseiam-se nas tecnologias disponíveis no momento de escrita desta Cartilha.

Uso indevido de recursos: um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar *spam*, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante.

Varredura: um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades (mais detalhes na Seção 3.2 do Capítulo Ataques na Internet).

Interceptação de tráfego: um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia (mais detalhes na Seção 3.4 do Capítulo Ataques na Internet).

Exploração de vulnerabilidades: por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como *modems* e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para *sites* fraudulentos.

Ataque de negação de serviço: um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar.

Ataque de força bruta: computadores conectados à rede e que usem senhas como método de autenticação, estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes.

Ataque de personificação: um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

Nas próximas seções são apresentados os cuidados gerais e independentes de tecnologia que você ter ao usar redes, os tipos mais comuns de acesso à Internet, os riscos adicionais que eles podem representar e algumas dicas de prevenção.

13.1 Cuidados gerais

Alguns cuidados que você deve tomar ao usar redes, independentemente da tecnologia, são:

- mantenha seu computador atualizado, com as versões mais recentes e com todas as atualizações aplicadas (mais detalhes no Capítulo Segurança de computadores);
- utilize e mantenha atualizados mecanismos de segurança, como programa *antimalware* e *firewall* pessoal (mais detalhes no Capítulo Mecanismos de segurança);
- seja cuidadoso ao elaborar e ao usar suas senhas (mais detalhes no Capítulo Contas e senhas);
- utilize conexão segura sempre que a comunicação envolver dados confidenciais (mais detalhes na Seção 10.1 do Capítulo Uso seguro da Internet);
- caso seu dispositivo permita o compartilhamento de recursos, desative esta função e somente a ative quando necessário e usando senhas difíceis de serem descobertas.

13.2 Wi-Fi

Wi-Fi (***Wi**reless **Fi**delity*) é um tipo de rede local que utiliza sinais de rádio para comunicação. Possui dois modos básicos de operação:

Infraestrutura: normalmente o mais encontrado, utiliza um concentrador de acesso (*Access Point* - AP) ou um roteador *wireless*.

Ponto a ponto (*ad-hoc*): permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP.

Redes Wi-Fi se tornaram populares pela mobilidade que oferecem e pela facilidade de instalação e de uso em diferentes tipos de ambientes. Embora sejam bastante convenientes, há alguns riscos que você deve considerar ao usá-las, como:

- por se comunicarem por meio de sinais de rádio, não há a necessidade de acesso físico a um ambiente restrito, como ocorre com as redes cabeadas. Devido a isto, os dados transmitidos por clientes legítimos podem ser interceptados por qualquer pessoa próxima com um mínimo de equipamento (por exemplo, um *notebook* ou *tablet*);
- por terem instalação bastante simples, muitas pessoas as instalam em casa (ou mesmo em empresas, sem o conhecimento dos administradores de rede), sem qualquer cuidado com configurações mínimas de segurança, e podem vir a ser abusadas por atacantes, por meio de uso não autorizado ou de "sequestro"[2];
- em uma rede Wi-Fi pública (como as disponibilizadas em aeroportos, hotéis e conferências) os dados que não estiverem criptografados podem ser indevidamente coletados por atacantes;
- uma rede Wi-Fi aberta pode ser propositadamente disponibilizada por atacantes para atrair usuários, a fim de interceptar o tráfego (e coletar dados pessoais) ou desviar a navegação para *sites* falsos.

Para resolver alguns destes riscos foram desenvolvidos mecanismos de segurança, como:

WEP (*Wired Equivalent Privacy*): primeiro mecanismo de segurança a ser lançado. É considerado frágil e, por isto, o uso deve ser evitado.

WPA (*Wi-Fi Protected Access*): mecanismo desenvolvido para resolver algumas das fragilidades do WEP. É o nível mínimo de segurança que é recomendado.

WPA-2: similar ao WPA, mas com criptografia considerada mais forte. É o mecanismo mais recomendado.

Cuidados a serem tomados:

- habilite a interface de rede Wi-Fi do seu computador ou dispositivo móvel somente quando usá-la e desabilite-a após o uso;

[2] Por sequestro de rede Wi-Fi entende-se uma situação em que um terceiro ganha acesso à rede e altera configurações no AP para que somente ele consiga acessá-la.

- desabilite o modo *ad-hoc* (use-o apenas quando necessário e desligue-o quando não precisar). Alguns equipamentos permitem inibir conexão com redes *ad-hoc*, utilize essa função caso o dispositivo permita;
- use, quando possível, redes que oferecem autenticação e criptografia entre o cliente e o AP (evite conectar-se a redes abertas ou públicas, sem criptografia, especialmente as que você não conhece a origem);
- considere o uso de criptografia nas aplicações, como por exemplo, PGP para o envio de *e-mails*, SSH para conexões remotas ou ainda VPNs;
- evite o acesso a serviços que não utilizem conexão segura ("https");
- evite usar WEP, pois ele apresenta vulnerabilidades que, quando exploradas, permitem que o mecanismo seja facilmente quebrado;
- use WPA2 sempre que disponível (caso seu dispositivo não tenha este recurso, utilize no mínimo WPA).

Cuidados ao montar uma rede sem fio doméstica:

- posicione o AP longe de janelas e próximo ao centro de sua casa a fim de reduzir a propagação do sinal e controlar a abrangência (conforme a potência da antena do AP e do posicionamento no recinto, sua rede pode abranger uma área muito maior que apenas a da sua residência e, com isto, ser acessada sem o seu conhecimento ou ter o tráfego capturado por vizinhos ou pessoas que estejam nas proximidades);
- altere as configurações padrão que acompanham o seu AP. Alguns exemplos são:
  - altere as senhas originais, tanto de administração do AP como de autenticação de usuários;
  - assegure-se de utilizar senhas bem elaboradas e difíceis de serem descobertas (mais detalhes no Capítulo Contas e senhas);
  - altere o SSID (***S**erver **S**et **ID**entifier*);
  - ao configurar o SSID procure não usar dados pessoais e nem nomes associados ao fabricante ou modelo, pois isto facilita a identificação de características técnicas do equipamento e pode permitir que essas informações sejam associadas a possíveis vulnerabilidades existentes;
  - desabilite a difusão (*broadcast*) do SSID, evitando que o nome da rede seja anunciado para outros dispositivos;
  - desabilite o gerenciamento do AP via rede sem fio, de tal forma que, para acessar funções de administração, seja necessário conectar-se diretamente a ele usando uma rede cabeada. Desta maneira, um possível atacante externo (via rede sem fio) não será capaz de acessar o AP para promover mudanças na configuração.
- não ative WEP, pois ele apresenta vulnerabilidades que, quando exploradas, permitem que o mecanismo seja facilmente quebrado;
- utilize WPA2 ou, no mínimo, WPA;

- caso seu AP disponibilize WPS (***W**i-Fi **P**rotected **S**etup*), desabilite-o a fim de evitar acessos indevidos;

- desligue seu AP quando não usar sua rede.

13.3 *Bluetooth*

Bluetooth é um padrão para tecnologia de comunicação de dados e voz, baseado em radiofrequência e destinado à conexão de dispositivos em curtas distâncias, permitindo a formação de redes pessoais sem fio. Está disponível em uma extensa variedade de equipamentos, como dispositivos móveis, videogames, *mouses*, teclados, impressoras, sistemas de áudio, aparelhos de GPS e monitores de frequência cardíaca. A quantidade de aplicações também é vasta, incluindo sincronismo de dados entre dispositivos, comunicação entre computadores e periféricos e transferência de arquivos.

Embora traga muitos benefícios, o uso desta tecnologia traz também riscos, visto que está sujeita às várias ameaças que acompanham as redes em geral, como varredura, furto de dados, uso indevido de recursos, ataque de negação de serviço, interceptação de tráfego e ataque de força bruta.

Um agravante, que facilita a ação dos atacantes, é que muitos dispositivos vêm, por padrão, com o *bluetooth* ativo. Desta forma, muitos usuários não percebem que possuem este tipo de conexão ativa e não se preocupam em adotar uma postura preventiva.

Cuidados a serem tomados:

- mantenha as interfaces *bluetooth* inativas e somente as habilite quando fizer o uso;

- configure as interfaces *bluetooth* para que a opção de visibilidade seja "Oculto" ou "Invisível", evitando que o nome do dispositivo seja anunciado publicamente. O dispositivo só deve ficar rastreável quando for necessário autenticar-se a um novo dispositivo ("pareamento");

- altere o nome padrão do dispositivo e evite usar na composição do novo nome dados que identifiquem o proprietário ou características técnicas do dispositivo;

- sempre que possível, altere a senha (PIN) padrão do dispositivo e seja cuidadoso ao elaborar a nova (mais detalhes no Capítulo Contas e senhas);

- evite realizar o pareamento em locais públicos, reduzindo as chances de ser rastreado ou interceptado por um atacante;

- fique atento ao receber mensagens em seu dispositivo solicitando autorização ou PIN (não responda à solicitação se não tiver certeza que está se comunicando com o dispositivo correto);

- no caso de perda ou furto de um dispositivo *bluetooth*, remova todas as relações de confiança já estabelecidas com os demais dispositivos que possui, evitando que alguém, de posse do dispositivo roubado/perdido, possa conectar-se aos demais.

13.4 Banda larga fixa

Banda larga fixa é um tipo de conexão à rede com capacidade acima daquela conseguida, usualmente, em conexão discada via sistema telefônico. Não há uma definição de métrica de banda larga que seja aceita por todos, mas é comum que conexões deste tipo sejam permanentes e não comutadas, como as discadas. Usualmente, compreende conexões com mais de 100 Kbps, porém esse limite é muito variável de país para país e de serviço para serviço[3].

Computadores conectados via banda larga fixa, geralmente, possuem boa velocidade de conexão, mudam o endereço IP com pouca frequência e ficam conectados à Internet por longos períodos. Por estas características, são visados por atacantes para diversos propósitos, como repositório de dados fraudulentos, para envio de *spam* e na realização de ataques de negação de serviço.

O seu equipamento de banda larga (*modem* ADSL, por exemplo) também pode ser invadido, pela exploração de vulnerabilidades ou pelo uso de senhas fracas e/ou padrão (facilmente encontradas na Internet). Caso um atacante tenha acesso ao seu equipamento de rede, ele pode alterar configurações, bloquear o seu acesso ou desviar suas conexões para *sites* fraudulentos.

Cuidados a serem tomados:

- altere, se possível, a senha padrão do equipamento de rede (verifique no contrato se isto é permitido e, caso seja, guarde a senha original e lembre-se de restaurá-la quando necessário);
- desabilite o gerenciamento do equipamento de rede via Internet (WAN), de tal forma que, para acessar funções de administração (interfaces de configuração), seja necessário conectar-se diretamente a ele usando a rede local (desta maneira, um possível atacante externo não será capaz de acessá-lo para promover mudanças na configuração).

13.5 Banda Larga Móvel

A banda larga móvel refere-se às tecnologias de acesso sem fio, de longa distância, por meio da rede de telefonia móvel, especialmente 3G e 4G[4].

Este tipo de tecnologia está disponível em grande quantidade de dispositivos móveis (como celulares, *smartphones* e *tablets*) e é uma das responsáveis pela popularização destes dispositivos e das redes sociais. Além disto, também pode ser adicionada a computadores e dispositivos móveis que ainda não tenham esta capacidade, por meio do uso de *modems* específicos.

Assim como no caso da banda larga fixa, dispositivos com suporte a este tipo de tecnologia podem ficar conectados à Internet por longos períodos e permitem que o usuário esteja *online*, independente de localização. Por isto, são bastante visados por atacantes para a prática de atividades maliciosas.

Cuidados a serem tomados:

- aplique os cuidados básicos de segurança, apresentados na Seção 13.1.

[3]Fonte: `http://www.cetic.br/`.

[4]3G e 4G correspondem, respectivamente, à terceira e quarta gerações de padrões de telefonia móvel definidos pela *International Telecommunication Union - ITU*.

14. Segurança em dispositivos móveis



Dispositivos móveis, como *tablets*, *smartphones*, celulares e PDAs, têm se tornado cada vez mais populares e capazes de executar grande parte das ações realizadas em computadores pessoais, como navegação *Web*, *Internet Banking* e acesso a *e-mails* e redes sociais. Infelizmente, as semelhanças não se restringem apenas às funcionalidades apresentadas, elas também incluem os riscos de uso que podem representar.

Assim como seu computador, o seu dispositivo móvel também pode ser usado para a prática de atividades maliciosas, como furto de dados, envio de *spam* e a propagação de códigos maliciosos, além de poder fazer parte de *botnets* e ser usado para disparar ataques na Internet.

Somadas a estes riscos, há características próprias que os dispositivos móveis possuem que, quando abusadas, os tornam ainda mais atraentes para atacantes e pessoas mal-intencionadas, como:

Grande quantidade de informações pessoais armazenadas: informações como conteúdo de mensagens SMS, lista de contatos, calendários, histórico de chamadas, fotos, vídeos, números de cartão de crédito e senhas costumam ficar armazenadas nos dispositivos móveis.

Maior possibilidade de perda e furto: em virtude do tamanho reduzido, do alto valor que podem possuir, pelo status que podem representar e por estarem em uso constante, os dispositivos móveis podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes.

Grande quantidade de aplicações desenvolvidas por terceiros: há uma infinidade de aplicações sendo desenvolvidas, para diferentes finalidades, por diversos autores e que podem facilmente ser obtidas e instaladas. Entre elas podem existir aplicações com erros de implementação, não confiáveis ou especificamente desenvolvidas para execução de atividades maliciosas.

Rapidez de substituição dos modelos: em virtude da grande quantidade de novos lançamentos, do desejo dos usuários de ter o modelo mais recente e de pacotes promocionais oferecidos pelas operadoras de telefonia, os dispositivos móveis costumam ser rapidamente substituídos e descartados, sem que nenhum tipo de cuidado seja tomado com os dados nele gravados.

De forma geral, os cuidados que você deve tomar para proteger seus dispositivos móveis são os mesmos a serem tomados com seu computador pessoal, como mantê-lo sempre atualizado e utilizar mecanismos de segurança. Por isto é muito importante que você siga as dicas apresentadas no Capítulo Segurança de computadores. Outros cuidados complementares a serem tomados são:

Antes de adquirir seu dispositivo móvel:

- considere os mecanismos de segurança que são disponibilizadas pelos diferentes modelos e fabricantes e escolha aquele que considerar mais seguro;
- caso opte por adquirir um modelo já usado, procure restaurar as configurações originais, ou "de fábrica", antes de começar a usá-lo;
- evite adquirir um dispositivo móvel que tenha sido ilegalmente desbloqueado (*jailbreak*) ou cujas permissões de acesso tenham sido alteradas. Esta prática, além de ser ilegal, pode violar os termos de garantia e comprometer a segurança e o funcionamento do aparelho.

Ao usar seu dispositivo móvel:

- se disponível, instale um programa *antimalware* antes de instalar qualquer tipo de aplicação, principalmente aquelas desenvolvidas por terceiros;
- mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas;
- fique atento às notícias veiculadas no *site* do fabricante, principalmente as relacionadas à segurança;
- seja cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e *plug-ins*. Procure usar aplicações de fontes confiáveis e que sejam bem avaliadas pelos usuários. Verifique comentários de outros usuários e se as permissões necessárias para a execução são coerentes com a destinação da aplicação (mais detalhes na Seção 6.4 do Capítulo Outros riscos);
- seja cuidadoso ao usar aplicativos de redes sociais, principalmente os baseados em geolocalização, pois isto pode comprometer a sua privacidade (mais detalhes na Seção 11.1 do Capítulo Privacidade).

Ao acessar redes[1]:

- seja cuidadoso ao usar redes Wi-Fi públicas;
- mantenha interfaces de comunicação, como *bluetooth*, infravermelho e Wi-Fi, desabilitadas e somente as habilite quando for necessário;
- configure a conexão *bluetooth* para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível").

Proteja seu dispositivo móvel e os dados nele armazenados:

- mantenha as informações sensíveis sempre em formato criptografado;
- faça *backups* periódicos dos dados nele gravados;
- mantenha controle físico sobre ele, principalmente em locais de risco (procure não deixá-lo sobre a mesa e cuidado com bolsos e bolsas quando estiver em ambientes públicos);
- use conexão segura sempre que a comunicação envolver dados confidenciais (mais detalhes na Seção 10.1 do Capítulo Uso seguro da Internet);
- não siga *links* recebidos por meio de mensagens eletrônicas;
- cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (alfanuméricas);
- configure-o para que seja localizado e bloqueado remotamente, por meio de serviços de geolocalização (isso pode ser bastante útil em casos de perda ou furto);
- configure-o, quando possível, para que os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso (use esta opção com bastante cautela, principalmente se você tiver filhos e eles gostarem de "brincar" com o seu dispositivo).

Ao se desfazer do seu dispositivo móvel:

- apague todas as informações nele contidas;
- restaure a opções de fábrica.

O que fazer em caso de perda ou furto:

- infome sua operadora e solicite o bloqueio do seu número (*chip*);
- altere as senhas que possam estar nele armazenadas (por exemplo, as de acesso ao seu *e-mail* ou rede social);
- bloqueie cartões de crédito cujo número esteja armazenado em seu dispositivo móvel;
- se tiver configurado a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados nele armazenados.

[1] Mais detalhes sobre estas dicas no Capítulo Segurança de redes.

Glossário

802.11 Conjunto de especificações desenvolvidas pelo IEEE para tecnologias de redes sem fio.

AC Veja Autoridade certificadora.

ADSL Do inglês ***A****symmetric* ***D****igital* ***S****ubscriber* ***L****ine*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um *modem* convencional.

Advance Fee Fraud
Veja Fraude de antecipação de recursos.

Adware Do inglês ***Ad****vertising* *Soft****ware***. Tipo específico de *spyware*. Programa projetado especificamente para apresentar propagandas. Pode ser usado de forma legítima, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

Antimalware Ferramenta que procura detectar e, então, anular ou remover os códigos maliciosos de um computador. Os programas antivírus, *antispyware*, *antirootkit* e *antitrojan* são exemplos de ferramentas *antimalware*.

Antivírus Tipo de ferramenta *antimalware* desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos. Pode incluir também a funcionalidade de *firewall* pessoal.

AP Do inglês ***A****ccess* ***P****oint*. Dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Artefato Qualquer informação deixada por um invasor em um sistema comprometido, como programas, *scripts*, ferramentas, *logs* e arquivos.

Assinatura digital
Código usado para comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada.

Atacante Pessoa responsável pela realização de um ataque. Veja também Ataque.

Ataque Qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede.

AUP Do inglês ***A**cceptable **U**se **P**olicy*. Veja Política de uso aceitável.

Autoridade certificadora
Entidade responsável por emitir e gerenciar certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

Backdoor Tipo de código malicioso. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim. Normalmente esse programa é colocado de forma a não a ser notado.

Banda, *Bandwidth*
Veja Largura de banda.

Banda larga Tipo de conexão à rede com capacidade acima daquela conseguida, usualmente, em conexão discada via sistema telefônico. Não há uma definição de métrica de banda larga que seja aceita por todos, mas é comum que conexões em banda larga sejam permanentes e não comutadas, como as conexões discadas. Usualmente, compreende conexões com mais de 100 Kbps, porém esse limite é muito variável de país para país e de serviço para serviço (Fonte: `http://www.cetic.br/`).

Banda larga fixa
Tipo de conexão banda larga que permite que um computador fique conectado à Internet por longos períodos e com baixa frequência de alteração de endereço IP.

Banda larga móvel
Tipo de conexão banda larga. Tecnologia de acesso sem fio, de longa distância, por meio de rede de telefonia móvel, especialmente 3G e 4G (respectivamente a terceira e a quarta geração de padrões de telefonia móvel definidos pelo *International Telecommunication Union* - ITU).

***Banner* de propaganda**
Espaço disponibilizado por um usuário em sua página *Web* para que serviços de publicidade apresentem propagandas de clientes.

Blacklist Lista de *e-mails*, domínios ou endereços IP, reconhecidamente fontes de *spam*. Recurso utilizado, tanto em servidores como em programas leitores de *e-mails*, para bloquear as mensagens suspeitas de serem *spam*.

Bluetooth Padrão para tecnologia de comunicação de dados e voz, baseado em radiofrequência e destinado à conexão de dispositivos em curtas distâncias, permitindo a formação de redes pessoais sem fio.

Boato Mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

Bot Tipo de código malicioso. Programa que, além de incluir funcionalidades de *worms*, dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. O processo de infecção e propagação do *bot* é similar ao do *worm*, ou seja, o *bot* é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. Veja também *Worm*.

Botnet Rede formada por centenas ou milhares de computadores infectados com *bots*. Permite potencializar as ações danosas executadas pelos *bots* e ser usada em ataques de negação de serviço, esquemas de fraude, envio de *spam*, etc. Veja também *Bot*.

Brute force Veja Força bruta.

Cable modem *Modem* projetado para operar sobre linhas de TV a cabo. Veja também *Modem*.

Cavalo de troia
Tipo de código malicioso. Programa normalmente recebido como um “presente” (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

Certificado digital
Registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um *site Web*) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

Certificado digital autoassinado
Certificado digital no qual o dono e o emissor são a mesma entidade.

Chave mestra Senha única usada para proteger (criptografar) outras senhas.

Código malicioso
Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*.

Código móvel Tipo de código utilizado por desenvolvedores *Web* para incorporar maior funcionalidade e melhorar a aparência de páginas *Web*. Alguns tipos de códigos móveis são: programas e *applets Java*, *JavaScripts* e componentes (ou controles) *ActiveX*.

Comércio eletrônico
Qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços por meio da Internet.

Comprometimento
Veja Invasão.

Computador zumbi
Nome dado a um computador infectado por *bot*, pois pode ser controlado remotamente, sem o conhecimento do seu dono. Veja também *Bot*.

Conexão discada
Conexão comutada à Internet, realizada por meio de um *modem* analógico e uma linha da rede de telefonia fixa, que requer que o *modem* disque um número telefônico para realizar o acesso (Fonte: http://www.cetic.br/).

Conexão segura
Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

Conta de usuário
Também chamada de "nome de usuário" e "nome de *login*". Corresponde à identificação única de um usuário em um computador ou serviço.

Cookie Pequeno arquivo que é gravado no computador quando o usuário acessa um *site* e reenviado a este mesmo *site* quando novamente acessado. É usado para manter informações sobre o usuário, como carrinho de compras, lista de produtos e preferências de navegação.

Correção de segurança
Correção desenvolvida para eliminar falhas de segurança em um programa ou sistema operacional.

Criptografia Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

DDoS Do inglês ***D**istributed **D**enial **o**f **S**ervice*. Veja Negação de serviço distribuído.

Defacement Veja Desfiguração de página.

Defacer Pessoa responsável pela desfiguração de uma página. Veja também Desfiguração de página.

Desfiguração de página
Também chamada de pichação. Técnica que consiste em alterar o conteúdo da página *Web* de um *site*.

Dispositivo móvel
Equipamento com recursos computacionais que, por ter tamanho reduzido, oferece grande mobilidade de uso, podendo ser facilmente carregado pelo seu dono. Exemplos: *notebooks*, *netbooks*, *tablets*, PDAs, *smartphones* e celulares.

DNS Do inglês ***D**omain **N**ame **S**ystem*. O sistema de nomes de domínios, responsável pela tradução, entre outros tipos, de nome de máquinas/domínios para o endereço IP correspondente e vice-versa.

DoS Do inglês ***D**enial **o**f **S**ervice*. Veja Negação de serviço.

E-commerce Veja Comércio eletrônico.

E-mail spoofing
Veja Falsificação de *e-mail*.

Endereço IP Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255, por exemplo, "`192.0.2.2`". No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF, por exemplo, "`2001:DB8:C001:900D:CA27:116A::1`".

Engenharia social
Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto desta Cartilha, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza engenharia social.

EV SSL Do inglês ***E**xtended **V**alidation **S**ecure **S**ocket **L**ayer*. Certificado SSL de Validação Avançada ou Estendida. Veja também SSL.

Exploit Veja Exploração de vulnerabilidade.

Exploração de vulnerabilidade
Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador. Veja também Vulnerabilidade.

Falsa identidade
Veja Furto de identidade.

Falsificação de *e-mail*
Técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Filtro *antispam*
Programa que permite separar os *e-mails* conforme regras pré-definidas. Utilizado tanto para o gerenciamento das caixas postais como para a seleção de *e-mails* válidos dentre os diversos *spams* recebidos.

Firewall Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.

***Firewall* pessoal**
Tipo específico de *firewall*. Programa usado para proteger um computador contra acessos não autorizados vindos da Internet.

Força bruta Tipo de ataque que consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios desse usuário.

Foursquare Rede social baseada em geolocalização que, assim como outras redes do mesmo tipo, utiliza os dados fornecidos pelo GPS do computador ou dispositivo móvel do usuário para registrar (fazer *check-in*) nos lugares por onde ele passa.

Fraude de antecipação de recursos
Tipo de fraude na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Função de resumo
Método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado *hash*.

Furto de identidade
Ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

GnuPG Conjunto de programas gratuito e de código aberto, que implementa criptografia de chave simétrica, de chaves assimétricas e assinatura digital.

Golpe de comércio eletrônico
Tipo de fraude na qual um golpista, com o objetivo de obter vantagens financeiras, explora a relação de confiança existente entre as partes envolvidas em uma transação comercial.

GPG Veja GnuPG.

Greylisting Método de filtragem de *spams*, implantado diretamente no servidor de *e-mails*, que recusa temporariamente um *e-mail* e o recebe somente quando ele é reenviado. Servidores legítimos de *e-mails*, que se comportam de maneira correta e de acordo com as especificações dos protocolos, sempre reenviam as mensagens. Este método parte do princípio que *spammers* raramente utilizam servidores legítimos e, portanto, não reenviam suas mensagens.

Harvesting Técnica utilizada por *spammers*, que consiste em varrer páginas *Web*, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*.

Hash Veja Função de resumo.

Hoax Veja Boato.

Hot fix Veja Correção de segurança.

HTML Do inglês ***H****yper****T****ext* ***M****arkup* ***L****anguage*. Linguagem universal utilizada na elaboração de páginas na Internet.

HTTP Do inglês ***H****yper****T****ext* ***T****ransfer* ***P****rotocol*. Protocolo usado para transferir páginas *Web* entre um servidor e um cliente (por exemplo, o navegador).

HTTPS Do inglês ***H****yper****T****ext* ***T****ransfer* ***P****rotocol* ***S****ecure* ou ***H****yper****T****ext* ***T****ransfer* ***P****rotocol over SSL*. Protocolo que combina o uso do HTTP com mecanismos de segurança, como o SSL e o TLS, a fim de prover conexões seguras. Veja também HTTP.

Identity theft Veja Furto de identidade.

IDS Do inglês ***I****ntrusion* ***D****etection* ***S****ystem*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

IEEE Acrônimo para ***I****nstitute of* ***E****lectrical and* ***E****lectronics* ***E****ngineers*, uma organização composta por engenheiros, cientistas e estudantes, que desenvolvem padrões para a indústria de computadores e eletroeletrônicos.

Incidente de segurança
Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Interceptação de tráfego
Técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

Invasão Ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

Invasor Pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão.

IP, IPv4, IPv6 Veja Endereço IP.

Janela de *pop-up*
Tipo de janela que aparece automaticamente e sem permissão, sobrepondo a janela do navegador *Web*, após o usuário acessar um *site*.

Keylogger Tipo específico de *spyware*. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*. Veja também *Spyware*.

Largura de banda
Quantidade de dados que podem ser transmitidos em um canal de comunicação, em um determinado intervalo de tempo.

***Link* curto** Tipo de *link* gerado por meio de serviços que transformam um *link* convencional em outro de tamanho reduzido. O *link* curto é automaticamente expandido para o *link* original, quando o usuário clica nele.

***Link* patrocinado**
Tipo de *link* apresentado em destaque em *site* de busca quando palavras específicas são pesquisadas pelo usuário. Quando o usuário clica em um *link* patrocinado, o *site* de busca recebe do anunciante um valor previamente combinado.

Log Registro de atividades gerado por programas e serviços de um computador. Termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo, de conexão (informações sobre a conexão de um computador à Internet) e de acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet).

Malvertising Do inglês ***Mal**icious ad**vertsing***. Tipo de golpe que consiste em criar anúncios maliciosos e, por meio de serviços de publicidade, apresentá-los em diversas páginas *Web*. Geralmente, o serviço de publicidade é induzido a acreditar que se trata de um anúncio legítimo e, ao aceitá-lo, intermedia a apresentação e faz com que ele seja mostrado em diversas páginas.

Malware Do inglês ***Mal**icious soft**ware***. Veja Código malicioso.

Master password
Veja Chave mestra.

MMS Do inglês ***M**ultimedia **M**essage **S**ervice*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de dados, como texto, imagem, áudio e vídeo.

Modem Do inglês ***Mo**dulator/**Dem**odulator*. Dispositivo responsável por converter os sinais do computador em sinais que possam ser transmitidos no meio físico de comunicação como, por exemplo, linha telefônica, cabo de TV, ar e fibra ótica.

Negação de serviço
Atividade maliciosa pela qual um atacante utiliza um computador ou dispositivo móvel para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Negação de serviço distribuído
Atividade maliciosa, coordenada e distribuída pela qual um conjunto de computadores e/ou dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Netiqueta Conjunto de normas de conduta para os usuários da Internet, definido no documento "RFC 1855: *Netiquette Guidelines*".

NTP Do inglês ***N****etwork* ***T****ime* ***P****rotocol*. Tipo de protocolo que permite a sincronização dos relógios dos dispositivos de uma rede, como servidores, estações de trabalho, roteadores e outros equipamentos, à partir de referências de tempo confiáveis (Fonte: http://ntp.br/).

Número IP Veja Endereço IP.

Opt-in Regra de envio de mensagens que define que é proibido mandar *e-mails* comerciais/*spam*, a menos que exista uma concordância prévia por parte do destinatário. Veja também *Soft opt-in*.

Opt-out Regra de envio de mensagens que define que é permitido mandar *e-mails* comerciais/*spam*, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

P2P Acrônimo para *peer-to-peer*. Arquitetura de rede onde cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, em que alguns dispositivos são dedicados a servir outros. Este tipo de rede é normalmente implementada via programas P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, etc.

Password Veja Senha.

Patch Veja Correção de segurança.

PGP Do inglês ***P****retty* ***G****ood* ***P****rivacy*. Programa que implementa criptografia de chave simétrica, de chaves assimétricas e assinatura digital. Possui versões comerciais e gratuitas. Veja também GnuPG.

Phishing*, *phishing scam*, *phishing/scam
Tipo de golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

***Plug-in*, complemento, extensão**
Programa geralmente desenvolvido por terceiros e que pode ser istalado no navegador *Web* e/ou programa leitor de *e-mails* para prover funcionalidades extras.

Política de segurança
Documento que define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra.

Política de uso aceitável
Também chamada de "Termo de Uso" ou "Termo de Serviço". Política na qual são definidas as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas.

Proxy Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar o desempenho de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. Quando mal configurado (*proxy* aberto) pode ser abusado por atacantes e utilizado para tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

***Proxy* aberto** *Proxy* mal configurado que pode ser abusado por atacantes e utilizado como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

PUA Veja Política de uso aceitável.

Rede sem fio Rede que permite a conexão entre computadores e outros dispositivos por meio da transmissão e recepção de sinais de rádio.

Rede Social Tipo de rede de relacionamento que permite que os usuários criem perfis e os utilizem para se conectar a outros usuários, compartilhar informações e se agrupar de acordo com interesses em comum. Alguns exemplos são: Facebook, Orkut, Twitter, Linkedin, Google+ e foursquare.

Rootkit Tipo de código malicioso. Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas, sim, para manter o acesso privilegiado em um computador previamente comprometido.

Scam Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan Veja Varredura em redes.

Scanner Programa usado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente usado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Screenlogger Tipo específico de *spyware*. Programa similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*. Veja também *Spyware*.

Senha Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser e que possui o direito de acessar o recurso em questão.

Service Pack Veja Correção de segurança.

Site Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

***Site* de compras coletivas**
Tipo de *site* por meio do qual os anunciantes ofertam produtos, normalmente com grandes descontos, por um tempo bastante reduzido e com quantidades limitadas. É considerado como intermediário entre as empresas que fazem os anúncios e os clientes que adquirem os produtos.

***Site* de leilão e venda de produtos**
Tipo de *site* que intermedia a compra e a venda de mercadorias entre os usuários. Alguns *sites* desse tipo oferecem sistema de gerenciamento por meio do qual o pagamento realizado pelo comprador somente é liberado ao vendedor quando a confirmação de que a mercadoria foi corretamente recebida é enviada.

S/MIME Do inglês ***S****ecure/****M****ultipurpose* ***I****nternet* ***M****ail* ***E****xtensions*. Padrão para assinatura e criptografia de *e-mails*.

SMS Do inglês ***S****hort* ***M****essage* ***S****ervice*. Tecnologia utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS, permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

SMTP Do inglês ***S****imple* ***M****ail* ***T****ransfer* ***P****rotocol*. Protocolo responsável pelo transporte de mensagens de *e-mail* na Internet.

Sniffer Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia. Veja também Interceptação de tráfego.

Sniffing Veja Interceptação de tráfego.

Soft opt-in Regra semelhante ao *opt-in*, mas neste caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Dessa forma, não é necessária a permissão explícita por parte do destinatário para receber *e-mails* desse remetente. Veja também *Opt-in*.

Spam Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.

Spam zombie Computador infectado por código malicioso (*bot*), capaz de transformar o sistema do usuário em um servidor de *e-mail* para envio de *spam*. Em muitos casos, o usuário do computador infectado demora a perceber que seu computador está sendo usado por um invasor para esse fim.

Spamcop Instituição que oferece diversos serviços *antispam*, sendo o mais conhecido o que permite reclamar automaticamente de *spams* recebidos.

Spammer Pessoa que envia *spam*.

Spyware Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger*, *screenlogger* e *adware* são alguns tipos específicos de *spyware*.

SSH Do inglês ***S****ecure* ***Sh****ell*. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

SSID Do inglês ***S****ervice* ***S****et* ***Id****entifier*. Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra, e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

SSL Do inglês ***S****ecure* ***S****ockets* ***L****ayer*. Assim como o TLS, é um protocolo que por meio de criptografia fornece confidencialidade e integridade nas comunicações entre um cliente e um servidor, podendo também ser usado para prover autenticação. Veja também HTTPS.

Time zone Fuso horário.

TLS Do inglês ***T****ransport* ***L****ayer* ***S****ecurity*. Assim como o SSL, é um protocolo que por meio de criptografia fornece confidencialidade e integridade nas comunicações entre um cliente e um servidor, podendo também ser usado para prover autenticação. Veja também HTTPS.

Trojan*, *Trojan horse
Veja Cavalo de troia.

UBE Do inglês ***U****nsolicited* ***B****ulk* ***E****-mail*. Termo usado para se referir aos *e-mails* não solicitados enviados em grande quantidade. Veja também *Spam*.

UCE Do inglês ***U****nsolicited* ***C****ommercial* ***E****-mail*. Termo usado para se referir aos *e-mails* comerciais não solicitados. Veja também *Spam*.

URL Do inglês ***U****niversal* ***R****esource* ***L****ocator*. Sequência de caracteres que indica a localização de um recurso na Internet como por exemplo, `http://cartilha.cert.br/`.

Username Veja Conta de usuário.

Varredura em redes
Técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados.

Vírus Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

VPN Do inglês ***V****irtual* ***P****rivate* ***N****etwork*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Vulnerabilidade
Condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Web bug Imagem, normalmente muito pequena e invisível, que faz parte de uma página *Web* ou de uma mensagem de *e-mail*, e que é projetada para monitorar quem está acessando esaa página *Web* ou mensagem de *e-mail*.

WEP Do inglês ***W****ired* ***E****quivalent* ***P****rivacy*. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados.

Whitelist Lista de *e-mails*, domínios ou endereços IP, previamente aprovados e que, normalmente, não são submetidos aos filtros *antispam* configurados.

Wi-Fi Do inglês ***Wi****reless* ***Fi****delity*. Marca registrada, genericamente usada para se referir a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless Veja Rede sem fio.

WLAN Do inglês ***W****ireless* ***L****ocal-****A****rea* ***N****etwork*. Tipo de rede que utiliza ondas de rádio de alta frequência, em vez de cabos, para a comunicação entre os computadores.

Worm Tipo de código malicioso. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores.

Zombie-computer
Veja Computador zumbi.

Índice Remissivo

T

V

W